7705 Service Aggregation Router

Release 23.10.R1

Log Events Guide

3HE 19516 AAAB TQZZA
Edition: 01
October 2023

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

1 Log Events

This chapter provides general information about the log events described in this guide.

For more information about log events and event logging, see the 7705 SAR System Management Guide.

Note: This guide contains all log events supported by the Service Router Operating System (SR OS). Not all events are supported by the 7705 SAR.

1.1 Overview of Log Events

Log events that are forwarded to a destination are formatted in a way that is appropriate for the specific destination; for example, whether it is to be recorded to a file or sent as an SNMP trap. However, log events also have common elements or properties. All application-generated events have the following properties:

- a timestamp in UTC or local time
- the generating application
- a unique event ID within the application
- a router name identifying the VRF ID that generated the event
- a subject identifying the affected object
- a short text description; for further information about variables found in the message format strings, see the associated SNMP Notification definition in the 7705 SAR MIBs

The general format for a log event with a memory, console, or file destination is as follows.

```
nnnn YYYY/MM/DD HH:MM:SS.SS TZONE <severity>: <application> #<event_id> <router-
name> <subject> <message>
```

The following is a log event example:

```
252 2017/05/07 16:21:00.76 UTC WARNING: SNMP #2005 Base my-interface-abc
"Interface my-interface-abc is operational"
```

The specific elements that make up the general format are described in the following table.

Table 1: Log Event Element Descriptions

Label	Description
nnnn	The log entry sequence number
YYYY/MM/DD	The UTC or local date stamp for the log entry *YYYY* — year *MM* — month

Label	Description
	DD — day
HH:MM:SS.SS	The UTC timestamp for the event *HH* — hours (24-hour format) *MM* — minutes *SS.SS* — seconds
TZONE	The timezone (for example, UTC, EDT) as configured by **configure log log-id** *log-id* **time-format**
<severity>	The severity level of the event • CRITICAL • MAJOR • MINOR • WARNING • INFO • CLEARED
<application>	The name of the application generating the log message
<event_id>	The application event ID number for the event
<router>	The router name representing the VRF ID that generated the event
<subject>	The subject/affected object for the event
<message>	A text description of the event

1.2 Log Event Example

The following table is a log event entry from this guide for the **cli_config_io** log event.

Table 2: cli_config_io properties

Property name	Value
Application name	L1
Event ID	2115
Event name	cli_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$: $prompt$ $message$*
Cause	A valid CLI command was entered in the configuration node.
Effect	Configuration was changed by CLI command.
Recovery	No recovery is required.

The table title for a log event entry is the event name. Each entry contains the information described in the following table.

Note: Not all log event entries have values in every field.

Table 3: Log Event Entry Field Descriptions

Label	Description
Application name	The name of the application generating the log message
Event ID	The application event ID number for the event
Event name	The name of the event
SNMP notification prefix and OID	The prefix and OID of the SNMP notification associated with the log event
Default severity	The default severity level of the event • CRITICAL • MAJOR • MINOR

Label	Description
	• WARNING • INFO • CLEARED
Message format string	A text description of the event
Cause	The cause of the event
Effect	The effect of the event
Recovery	How to recover from this event, if necessary

2 APPLICATION_ASSURANCE

2.1 tmnxBsxAarpInstOperStateChanged

Table 4: tmnxBsxAarpInstOperStateChanged properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4435
Event name	tmnxBsxAarpInstOperStateChanged
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.35
Default severity	warning
Message format string	Status of AARP instance *$tmnxBsxAarpInstId$* changed operational state: *$tmnxBsxAarpInstOperState$*, flags = *$tmnxBsxAarpInstOperFlags$*
Cause	A tmnxBsxAarpInstOperStateChanged notification is generated when the operational state of the AARP instance changes.
Effect	The transition to an operational state of 'outOfService(3)' indicates that the AARP instance is not performing asymmetry removal.
Recovery	No recovery is required.

2.2 tmnxBsxAarpInstStateChanged

Table 5: tmnxBsxAarpInstStateChanged properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4436
Event name	tmnxBsxAarpInstStateChanged
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.36
Default severity	warning

Property name	Value
Message format string	Status of AARP instance *$tmnxBsxAarpInstId$* changed state: *$tmnx BsxAarpInstState$*, flags = *$tmnxBsxAarpInstOperFlags$*
Cause	A tmnxBsxAarpInstStateChanged notification is generated when the state of the AARP instance changes.
Effect	None.
Recovery	No recovery is required.

2.3 tmnxBsxAaSubPolResExceeded

Table 6: tmnxBsxAaSubPolResExceeded properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4413
Event name	tmnxBsxAaSubPolResExceeded
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.13
Default severity	warning
Message format string	Policer resources have been exceeded for subscribers in group *$tmnx BsxNotifyAaGrpPartIndex$*.
Cause	A tmnxBsxAaSubPolResExceeded notification is generated when Application Assurance policer resources have been exceeded for subscribers with the ISA-AA group and partition.
Effect	Subscriber policing is degraded.
Recovery	Recovery from this condition requires the reconfiguration of subscriber policy to reduce the number of policers being applied.

2.4 tmnxBsxAaSubPolResExceededClear

Table 7: tmnxBsxAaSubPolResExceededClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4414

Property name	Value
Event name	tmnxBsxAaSubPolResExceededClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.14
Default severity	warning
Message format string	Policer resources are no longer exceeded for subscribers in group *$tmnxBsxNotifyAaGrpPartIndex$*.
Cause	A tmnxBsxAaSubPolResExceededClear notification is generated when Application Assurance policer resources are no longer exceeded for subscribers with the ISA-AA group and partition.
Effect	Policer resources are no longer exceeded for subscribers.
Recovery	None.

2.5 tmnxBsxAaSubscriberAcctDataLoss

Table 8: tmnxBsxAaSubscriberAcctDataLoss properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4412
Event name	tmnxBsxAaSubscriberAcctDataLoss
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.12
Default severity	warning
Message format string	Accounting data loss occurred for subscriber *$tmnxBsxNotify AaSubscriberName$*.
Cause	A tmnxBsxAaSubscriberAcctDataLoss notification is generated when Application Assurance subscriber statistics cannot be written to the accounting file. This can occur if the accounting interval expires while collecting statistics.
Effect	When this notification is generated it signifies that the statistic records, for this application assurance subscriber, are missing from the accounting file for the indicated interval.
Recovery	No recovery is required.

2.6 tmnxBsxAaSubscribersUnassigned

Table 9: tmnxBsxAaSubscribersUnassigned properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4411
Event name	tmnxBsxAaSubscribersUnassigned
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.11
Default severity	warning
Message format string	ISA-AA group *$tmnxBsxNotifyIsaAaGroupIndex$* has unassigned subscribers
Cause	A tmnxBsxAaSubscribersUnassigned notification is generated when one or more subscribers for a particular service-id cannot be assigned to an ISA-AA MDA within an Application Assurance group due to insufficient resources. The resources in question include service queues, AA subscriber counts or AA subscriber statistics.
Effect	Unassigned subscribers will behave as specified by the fail-to mode configured within the Application Assurance group.
Recovery	Recovery from this condition requires the removal and re-creation of the AA subscribers when sufficient resources become available.

2.7 tmnxBsxDatapathCpuUsage

Table 10: tmnxBsxDatapathCpuUsage properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4458
Event name	tmnxBsxDatapathCpuUsage
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.58
Default severity	minor
Message format string	Datapath CPU usage is greater than or equal to *$tmnxBsxDatapath CpuHighWatermark$*% on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* in group *$tmnxBsxNotifyIsaAaGroupIndex$*.

Property name	Value
Cause	A tmnxBsxDatapathCpuUsage notification is generated when the current datapath CPU usage on the MDA in the ISA-AA group is greater than or equal to the tmnxBsxDatapathCpuHighWatermark and the prior usage was less than this threshold.
Effect	There is no immediate effect, but when the usage hits the limit of 100%, traffic will be dropped unless the value of tmnxBsxIsaAaGrpOverload CutThru is 'enabled (1)' for the Application Assurance group.
Recovery	There is no recovery for this notification.

2.8 tmnxBsxDatapathCpuUsageClear

Table 11: tmnxBsxDatapathCpuUsageClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4459
Event name	tmnxBsxDatapathCpuUsageClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.59
Default severity	minor
Message format string	Datapath CPU usage is less than or equal to *$tmnxBsxDatapathCpu LowWatermark$*% on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* in group *$tmnxBsxNotifyIsaAaGroupIndex$*.
Cause	A tmnxBsxDatapathCpuUsageClear notification is generated to indicate a prior tmnxBsxDatapathCpuUsage notification has cleared due to the current datapath CPU usage on the MDA in the ISA-AA group being less than or equal to the tmnxBsxDatapathCpuLowWatermark.
Effect	The tmnxBsxDatapathCpuUsage notification is cleared.
Recovery	There is no recovery for this notification.

2.9 tmnxBsxDnsIpCacheFull

Table 12: tmnxBsxDnsIpCacheFull properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4444
Event name	tmnxBsxDnsIpCacheFull
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.44
Default severity	minor
Message format string	The usage of ISA-AA Group *$tmnxBsxIsaAaGroupIndex$* DNS IP Cache "*$tmnxBsxDnsIpCacheName$*" for ISA-MDA *$tmnxBsxNotify ActiveMda$* is greater than or equal to the *$tmnxBsxDnsIpCache HighWatermark$*% high watermark. The cache size is *$tmnxBsxDns IpCacheSize$*.
Cause	A tmnxBsxDnsIpCacheFull notification is generated when the number of entries in a DNS IP Cache is greater than or equal to the percentage value tmnxBsxDnsIpCacheHighWatermark of its tmnxBsxDnsIpCache Size and the previous percentage value was less than this threshold.
Effect	The DNS IP Cache is relatively close to being full.
Recovery	The notification can be cleared if enough cache entries timeout to drop below the threshold, or if the cache is cleared, or tmnxBsxDnsIpCache Size is sufficiently increased.

2.10 tmnxBsxDnsIpCacheFullClear

Table 13: tmnxBsxDnsIpCacheFullClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4445
Event name	tmnxBsxDnsIpCacheFullClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.45
Default severity	minor
Message format string	The usage of ISA-AA Group *$tmnxBsxIsaAaGroupIndex$* DNS IP Cache "*$tmnxBsxDnsIpCacheName$*" for ISA-MDA *$tmnxBsxNotify ActiveMda$* is less than or equal to the *$tmnxBsxDnsIpCacheLow*

Property name	Value
	Watermark$*% low watermark. The cache size is *$tmnxBsxDnsIpCacheSize$.
Cause	A tmnxBsxDnsIpCacheFullClear notification is generated when the number of entries in a DNS IP Cache is less than or equal to the percentage value tmnxBsxDnsIpCacheLowWatermark of its tmnxBsxDnsIpCacheSize and the previous percentage value was greater than this threshold.
Effect	The DNS IP Cache is no longer relatively close to being full.
Recovery	No recovery is required.

2.11 tmnxBsxHttpUrlParamLimitExceeded

Table 14: tmnxBsxHttpUrlParamLimitExceeded properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4441
Event name	tmnxBsxHttpUrlParamLimitExceeded
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.41
Default severity	minor
Message format string	Subscriber HTTP URL Parameter storage has been exceeded for subscribers in group *$tmnxBsxNotifyIsaAaGroupIndex$*, reason: *$tmnxBsxNotifyReason$*
Cause	A tmnxBsxHttpUrlParamLimitExceeded notification is generated when the group limit of unique tmnxBsxAaSubHttpUrlParam values has been exceeded. The tmnxBsxNotifyReason will identify the reason this notification was raised.
Effect	Some subscribers will not have their HTTP URL Parameters applied.
Recovery	No recovery is required.

2.12 tmnxBsxIsaAaGrpBitRate

Table 15: tmnxBsxIsaAaGrpBitRate properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4419
Event name	tmnxBsxIsaAaGrpBitRate
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.19
Default severity	warning
Message format string	Bit rate is greater than or equal to *$tmnxBsxBitRateHighWatermark$* megabits/s on ISA-AA MDA *$tmnxBsxNotifyActiveMda$*.
Cause	A tmnxBsxIsaAaGrpBitRate notification is generated when the current bit rate on the MDA in the ISA-AA group is greater than or equal to the tmnxBsxBitRateHighWatermark and the prior rate was less than this threshold.
Effect	None.
Recovery	No recovery is required.

2.13 tmnxBsxIsaAaGrpBitRateClear

Table 16: tmnxBsxIsaAaGrpBitRateClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4420
Event name	tmnxBsxIsaAaGrpBitRateClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.20
Default severity	warning
Message format string	Bit rate is less than or equal to *$tmnxBsxBitRateLowWatermark $* megabits/s on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* or corresponding tmnxBsxIsaAaGrpBitRate notification has been disabled.
Cause	A tmnxBsxIsaAaGrpBitRateClear notification is generated to indicate a prior tmnxBsxIsaAaGrpBitRate notification has cleared due to one of the following reasons: 1. The current bit rate on the MDA in the ISA-

Property name	Value
	AA group is less than or equal to the tmnxBsxBitRateLowWatermark. 2. The corresponding tmnxBsxIsaAaGrpBitRate notification has been disabled raising the tmnxBsxBitRateHighWatermark to maximum.
Effect	None.
Recovery	No recovery is required.

2.14 tmnxBsxIsaAaGrpCapCostThres

Table 17: tmnxBsxIsaAaGrpCapCostThres properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4409
Event name	tmnxBsxIsaAaGrpCapCostThres
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.9
Default severity	warning
Message format string	The capacity cost on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* in ISA-AA Group *$tmnxBsxIsaAaGroupIndex$* is greater than or equal to the high threshold *$tmnxBsxIsaAaGrpCapCostHighThres$*
Cause	A tmnxBsxIsaAaGrpCapCostThres notification is generated when the current capacity cost for an MDA within an ISA-AA Group is greater than or equal to the threshold specified by tmnxBsxIsaAaGrpCapCost HighThres and the prior cost was less than this threshold.
Effect	There is no direct adverse effect, however this may indicate that resources are limited. Exhaustion of resources will cause new aa-sub assignment to fail.
Recovery	If resource availability is sufficient, the capacity cost threshold can be increased or the app-profile capacity cost configuration can be reduced. If resources are limited and need to be recovered, remove aa-subs, or add additional isa-aa cards to the group.

2.15 tmnxBsxIsaAaGrpCapCostThresClear

Table 18: tmnxBsxIsaAaGrpCapCostThresClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4410
Event name	tmnxBsxIsaAaGrpCapCostThresClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.10
Default severity	warning
Message format string	The capacity cost on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* in ISA-AA Group *$tmnxBsxIsaAaGroupIndex$* is less than or equal to the low threshold *$tmnxBsxIsaAaGrpCapCostLowThres$*
Cause	A tmnxBsxIsaAaGrpCapCostThresClear notification is generated when the current capacity cost for an MDA within an ISA-AA Group is less than or equal to the threshold specified by tmnxBsxIsaAaGrpCapCost LowThres and the prior cost was greater than this threshold.
Effect	None.
Recovery	No recovery is required.

2.16 tmnxBsxIsaAaGrpFailureClearV2

Table 19: tmnxBsxIsaAaGrpFailureClearV2 properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4402
Event name	tmnxBsxIsaAaGrpFailureClearV2
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.6
Default severity	warning
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* recovered
Cause	All configured ISA-AA MDAs are in service.
Effect	Service is fully restored.
Recovery	No recovery is required.

2.17 tmnxBsxIsaAaGrpFailureV2

Table 20: tmnxBsxIsaAaGrpFailureV2 properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4401
Event name	tmnxBsxIsaAaGrpFailureV2
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.5
Default severity	major
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* failed
Cause	The ISA-AA Group has no configured primary MDA or the number of active MDAs is not equal to the number of configured primary MDAs.
Effect	Traffic that was to be diverted to the ISA-AA Group will instead have the rule specified in TIMETRA-BSX-NG-MIB::tmnxBsxIsaAaGrpFail ToMode applied to it.
Recovery	No recovery is required.

2.18 tmnxBsxIsaAaGrpFlowFull

Table 21: tmnxBsxIsaAaGrpFlowFull properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4405
Event name	tmnxBsxIsaAaGrpFlowFull
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.3
Default severity	major
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* flow record usage is greater than or equal to high watermark. The Active ISA-AA MDA is *$tmnxBsxNotifyActiveMda$*
Cause	Excessive traffic including denial of service attacks that target flow state exhaustion

Property name	Value
Effect	Traffic that is unable to allocate a flow record is treated using policy defined for the subscriber for an "Unknown" protocol.
Recovery	No recovery is required.

2.19 tmnxBsxIsaAaGrpFlowFullClear

Table 22: tmnxBsxIsaAaGrpFlowFullClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4407
Event name	tmnxBsxIsaAaGrpFlowFullClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.4
Default severity	warning
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* flow record usage is less than or equal to low watermark. The Active ISA-AA MDA is *$tmnx BsxNotifyActiveMda$*
Cause	The conditions that caused tmnxBsxIsaAaGrpFlowFull or tmnxBsxIsa AaGrpFlowFull have been alleviated.
Effect	None.
Recovery	No recovery is required.

2.20 tmnxBsxIsaAaGrpFlowSetup

Table 23: tmnxBsxIsaAaGrpFlowSetup properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4415
Event name	tmnxBsxIsaAaGrpFlowSetup
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.15
Default severity	warning

Property name	Value
Message format string	Flow setup rate is greater than or equal to *$tmnxBsxFlowSetupHigh Watermark$* flows/s on ISA-AA MDA *$tmnxBsxNotifyActiveMda$*.
Cause	A tmnxBsxIsaAaGrpFlowSetup notification is generated when the current flow setup rate on the MDA in the ISA-AA group is greater than or equal to tmnxBsxFlowSetupHighWatermark and the prior rate was less than this threshold.
Effect	None.
Recovery	No recovery is required.

2.21 tmnxBsxIsaAaGrpFlowSetupClear

Table 24: tmnxBsxIsaAaGrpFlowSetupClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4416
Event name	tmnxBsxIsaAaGrpFlowSetupClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.16
Default severity	warning
Message format string	Flow setup rate is less than or equal to *$tmnxBsxFlowSetupLow Watermark$* flows/s on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* or corresponding tmnxBsxIsaAaGrpFlowSetup notification has been disabled.
Cause	A tmnxBsxIsaAaGrpFlowSetupClear notification is generated to indicate a prior tmnxBsxIsaAaGrpFlowSetup notification has cleared due to one of the following reasons: 1. The current flow setup rate on the MDA in the ISA-AA group is less than or equal to tmnxBsxFlow SetupLowWatermark. 2. The corresponding tmnxBsxIsaAaGrpFlow Setup notification has been disabled by raising the tmnxBsxFlowSetup HighWatermark to maximum.
Effect	None.
Recovery	No recovery is required.

2.22 tmnxBsxIsaAaGrpFmSbWaSBufOvld

Table 25: tmnxBsxIsaAaGrpFmSbWaSBufOvld properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4428
Event name	tmnxBsxIsaAaGrpFmSbWaSBufOvld
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.28
Default severity	warning
Message format string	ISA-AA group *$tmnxBsxIsaAaGroupIndex$* MDA *$tmnxBsxNotifyActiveMda$* wa-shared buffer use is greater than or equal to *$tmnxBsxIsaAaGrpFromSubWaSBfHiWmk$* in the from-subscriber direction.
Cause	A tmnxBsxIsaAaGrpFmSbWaSBufOvld is generated when the current weighted average shared buffer use for an ISA in the from-subscriber direction is greater than or equal to a high watermark after being in a normal, non-overloaded, state.
Effect	If ISA overload cut-through is enabled, the ISA MDA performs subscriber level cut-through of all traffic.
Recovery	No recovery is required.

2.23 tmnxBsxIsaAaGrpFmSbWaSBufOvldClr

Table 26: tmnxBsxIsaAaGrpFmSbWaSBufOvldClr properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4429
Event name	tmnxBsxIsaAaGrpFmSbWaSBufOvldClr
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.29
Default severity	warning
Message format string	ISA-AA group *$tmnxBsxIsaAaGroupIndex$* MDA *$tmnxBsxNotifyActiveMda$* wa-shared buffer use is less than or equal to *$tmnxBsxIsaAaGrpFromSubWaSBfLoWmk$* in the from-subscriber direction or corresponding tmnxBsxIsaAaGrpFmSbWaSBufOvld notification has been disabled.

Property name	Value
Cause	A tmnxBsxIsaAaGrpFmSbWaSBufOvldClr is generated to indicate a prior tmnxBsxIsaAaGrpFmSbWaSBufOvld notification has cleared due to one of the following reasons: 1. The current weighted average shared buffer use in the from-subscriber direction is less than or equal to a low watermark. 2. The corresponding tmnxBsxIsaAaGrpFmSb WaSBufOvld notification has been disabled by raising the tmnxBsxIsa AaGrpFromSubWaSBfHiWmk to maximum.
Effect	The buffer pool in the from-subscriber direction exits overload. ISA MDA overload cut-through ends if it was in effect and the buffer pools in both directions are no longer overloaded.
Recovery	No recovery is required.

2.24 tmnxBsxIsaAaGrpNonRedundantV2

Table 27: tmnxBsxIsaAaGrpNonRedundantV2 properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4403
Event name	tmnxBsxIsaAaGrpNonRedundantV2
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.7
Default severity	minor
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* has a backup MDA configured, but has no standby MDA available.
Cause	The ISA-AA Group has a configured backup MDA but there is no standby MDA available.
Effect	Traffic is diverted but in the event of a failure of any of the active ISA-AA MDAs, there is no backup ISA-AA MDA to take over.
Recovery	No recovery is required.

2.25 tmnxBsxIsaAaGrpOvrldCutthru

Table 28: tmnxBsxIsaAaGrpOvrldCutthru properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4432
Event name	tmnxBsxIsaAaGrpOvrldCutthru
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.32
Default severity	warning
Message format string	ISA AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* MDA *$tmnxBsxNotifyActiveMda$* entering overload cut through processing.
Cause	A tmnxBsxIsaAaGrpOvrldCutthru is generated when cut through processing starts on an ISA MDA.
Effect	The ISA MDA performs subscriber level cut-through of all traffic.
Recovery	No recovery is required.

2.26 tmnxBsxIsaAaGrpOvrldCutthruClr

Table 29: tmnxBsxIsaAaGrpOvrldCutthruClr properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4433
Event name	tmnxBsxIsaAaGrpOvrldCutthruClr
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.33
Default severity	warning
Message format string	ISA AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* MDA *$tmnxBsxNotifyActiveMda$* exiting overload cut through processing.
Cause	A tmnxBsxIsaAaGrpOvrldCutthru is generated when cut through processing ends on an ISA MDA.
Effect	The ISA MDA stops performing subscriber level cut-through of all traffic.
Recovery	No recovery is required.

2.27 tmnxBsxIsaAaGrpPacketRate

Table 30: tmnxBsxIsaAaGrpPacketRate properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4417
Event name	tmnxBsxIsaAaGrpPacketRate
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.17
Default severity	warning
Message format string	Packet rate is greater than or equal to *$tmnxBsxPacketRateHigh Watermark$* packets/s on ISA-AA MDA *$tmnxBsxNotifyActiveMda$*.
Cause	A tmnxBsxIsaAaGrpPacketRate notification is generated when the current packet rate on the MDA in the ISA-AA group is greater than or equal to the tmnxBsxPacketRateHighWatermark and the prior rate was less than this threshold.
Effect	None.
Recovery	No recovery is required.

2.28 tmnxBsxIsaAaGrpPacketRateClear

Table 31: tmnxBsxIsaAaGrpPacketRateClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4418
Event name	tmnxBsxIsaAaGrpPacketRateClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.18
Default severity	warning
Message format string	Packet rate is less than or equal to *$tmnxBsxPacketRateLow Watermark$* packets/s on ISA-AA MDA *$tmnxBsxNotifyActiveMda$* or corresponding tmnxBsxIsaAaGrpPacketRate notification has been disabled.

Property name	Value
Cause	A tmnxBsxIsaAaGrpPacketRateClear notification is generated to indicate a prior tmnxBsxIsaAaGrpPacketRate notification has cleared due to one of the following reasons: 1. The current packet rate on the MDA in the ISA-AA group is less than or equal to the tmnxBsxPacket RateLowWatermark. 2. The corresponding tmnxBsxIsaAaGrpPacket Rate notification has been disabled by raising the tmnxBsxPacketRate HighWatermark to maximum.
Effect	None.
Recovery	No recovery is required.

2.29 tmnxBsxIsaAaGrpSwitchover

Table 32: tmnxBsxIsaAaGrpSwitchover properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4404
Event name	tmnxBsxIsaAaGrpSwitchover
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.2
Default severity	warning
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* has switched activity. The Active ISA-AA MDA is now *$tmnxBsxNotifyActiveMda$*
Cause	Other events will show the reason that the activity switch occurred.
Effect	A small amount of traffic may be lost during the activity switch.
Recovery	No recovery is required.

2.30 tmnxBsxIsaAaGrpToSbWaSBufOvld

Table 33: tmnxBsxIsaAaGrpToSbWaSBufOvld properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4430

Property name	Value
Event name	tmnxBsxIsaAaGrpToSbWaSBufOvId
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.30
Default severity	warning
Message format string	ISA-AA group *$tmnxBsxIsaAaGroupIndex$* MDA *$tmnxBsxNotifyActiveMda$* wa-shared buffer use is greater than or equal to *$tmnxBsxIsaAaGrpToSubWaSBfHiWmk$* in the to-subscriber direction.
Cause	A tmnxBsxIsaAaGrpToSbWaSBufOvId is generated when the current weighted average shared buffer use for an ISA in the to-subscriber direction is greater than or equal to a high watermark after being in a normal, non-overloaded, state.
Effect	If ISA overload cut through is enabled, the ISA MDA performs subscriber level cut-through of all traffic.
Recovery	No recovery is required.

2.31 tmnxBsxIsaAaGrpToSbWaSBufOvIdClr

Table 34: tmnxBsxIsaAaGrpToSbWaSBufOvIdClr properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4431
Event name	tmnxBsxIsaAaGrpToSbWaSBufOvIdClr
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.31
Default severity	warning
Message format string	ISA-AA group *$tmnxBsxIsaAaGroupIndex$* MDA *$tmnxBsxNotifyActiveMda$* wa-shared buffer use is less than or equal to *$tmnxBsxIsaAaGrpToSubWaSBfLoWmk$* in the to-subscriber direction or corresponding tmnxBsxIsaAaGrpToSbWaSBufOvId notification has been disabled.
Cause	A tmnxBsxIsaAaGrpToSbWaSBufOvIdClr is generated to indicate a prior tmnxBsxIsaAaGrpToSbWaSBufOvId notification has cleared due to one of the following reasons: 1. The weighted average shared buffer use for an ISA in the to-subscriber direction is less than or equal to a low watermark. 2. The corresponding tmnxBsxIsaAaGrpToSbWaSBufOvId notification has been disabled by raising the tmnxBsxIsaAaGrpToSubWaSBfHiWmk to maximum.

Property name	Value
Effect	The buffer pool in the to-subscriber direction exits overload. ISA MDA overload cut-through ends if it was in effect and the buffer pools in both directions are no longer overloaded.
Recovery	No recovery is required.

2.32 tmnxBsxIsaAaSubLoadBalance

Table 35: tmnxBsxIsaAaSubLoadBalance properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4408
Event name	tmnxBsxIsaAaSubLoadBalance
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.8
Default severity	warning
Message format string	Subscriber load-balancing operation for ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$*, *$tmnxBsxNotifyActionStatus$*
Cause	Triggered by an operator.
Effect	A small amount of traffic may be lost for balanced subscribers.
Recovery	No recovery is required.

2.33 tmnxBsxIsaAaTimFileProcFailure

Table 36: tmnxBsxIsaAaTimFileProcFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4448
Event name	tmnxBsxIsaAaTimFileProcFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.48
Default severity	minor

Property name	Value
Message format string	Failed to process isa-aa.tim file with reason: *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxIsaAaTimFileProcFailure notification is generated when a problem is encountered while attempting to process the isa-aa.tim file from the boot options file (BOF) images directory. The tmnxBsxNotify Reason will identify the reason this notification was raised.
Effect	The isa-aa.tim file cannot be processed.
Recovery	Based on the reason noted in tmnxBsxNotifyReason, if necessary take action to ensure that a valid isa-aa.tim file, compatible with the running CPM software version, is located in the images directory configured in the BOF. If successive attempts to load the isa-aa.tim fail, please contact Nokia customer support.

2.34 tmnxBsxMobileSubModifyFailure

Table 37: tmnxBsxMobileSubModifyFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4439
Event name	tmnxBsxMobileSubModifyFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.39
Default severity	minor
Message format string	Failed to modify a subscriber in group *$tmnxBsxNotifyAaGrpPartIndex$* with reason: *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxMobileSubModifyFailure notification is generated when attempting to apply an override (app-profile or ASO) to a subscriber based on information received from the ISA-MG. The tmnxBsxNotify Reason will identify the reason this trap was raised.
Effect	The override will not be applied to the subscriber.
Recovery	Based on the reason noted in tmnxBsxNotifyReason, if necessary take action to ensure that a configuration mis-match has not occurred to allow the overrides to be applied appropriately.

2.35 tmnxBsxRadApFailure

Table 38: tmnxBsxRadApFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4437
Event name	tmnxBsxRadApFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.37
Default severity	warning
Message format string	A RADIUS accounting request failed to be sent to any of the RADIUS servers in accounting policy *$tmnxBsxRadApName$* with reason: *$tmnxBsxNotifyReason$*.
Cause	The tmnxBsxRadApFailure notification is generated when a RADIUS accounting request was not successfully sent to any of the RADIUS servers in the accounting policy.
Effect	Accounting data for current subscribers will not be exported externally.
Recovery	Based on the reason noted in tmnxBsxNotifyReason, if necessary take action to ensure that the next RADIUS accounting request will be successfully sent.

2.36 tmnxBsxRadApIntrmUpdateSkipped

Table 39: tmnxBsxRadApIntrmUpdateSkipped properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4440
Event name	tmnxBsxRadApIntrmUpdateSkipped
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.40
Default severity	minor
Message format string	Interim update interval, configured as *$tmnxBsxRadApIntrmUpdate Interval$* minutes, has been ignored.

Property name	Value
Cause	The tmnxBsxRadApIntrmUpdateSkipped notification is generated when an interim update has been triggered while subscriber accounting information is still being sent for the previous interim update interval.
Effect	Accounting data for this interim update will not be sent.
Recovery	If this continues to occur consider increasing the RADIUS Accounting interim update interval (tmnxBsxRadApIntrmUpdateInterval).

2.37 tmnxBsxRadApServOperStateChange

Table 40: tmnxBsxRadApServOperStateChange properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4438
Event name	tmnxBsxRadApServOperStateChange
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.38
Default severity	warning
Message format string	AA RADIUS accounting policy *$tmnxBsxRadApName$* server *$tmnx BsxRadApServIndex$* address *$tmnxBsxRadApServAddr$* state changed to *$tmnxBsxRadApServOperState$*.
Cause	The tmnxBsxRadApServOperStateChange notification is generated when the operational status of an AA RADIUS accounting policy server has transitioned either from 'inService' to 'outOfService' or from 'out OfService' to 'inService'.
Effect	None.
Recovery	No recovery is required.

2.38 tmnxBsxStatFtrEnTcaThreshCrClear

Table 41: tmnxBsxStatFtrEnTcaThreshCrClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4456

Property name	Value
Event name	tmnxBsxStatFtrEnTcaThreshCrClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.56
Default severity	minor
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotify AaGrpPartIndex$ $tmnxBsxNotifyTcaCfgFilterType$* " *$tmnxBsxNotify TcaCfgFilterName$*" entry *$tmnxBsxNotifyTcaFtrEnCfgEntryId$* in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatFtrEnTcaThreshCrClear notification is generated when the utilization matching a tmnxBsxStatTcaFtrEnCfgEntry in the past minute is less than or equal to the value of tmnxBsxStatTcaFtrEnCfg LoWmark and tmnxBsxStatFtrEnTcaThreshCrossed is currently raised. The tmnxBsxNotifyReason will identify the utilization.
Effect	The tmnxBsxStatFtrEnTcaThreshCrossed notification is cleared.
Recovery	There is no recovery for this notification.

2.39 tmnxBsxStatFtrEnTcaThreshCrossed

Table 42: tmnxBsxStatFtrEnTcaThreshCrossed properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4455
Event name	tmnxBsxStatFtrEnTcaThreshCrossed
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.55
Default severity	minor
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotify AaGrpPartIndex$ $tmnxBsxNotifyTcaCfgFilterType$* " *$tmnxBsxNotify TcaCfgFilterName$*" entry *$tmnxBsxNotifyTcaFtrEnCfgEntryId$* in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatFtrEnTcaThreshCrossed notification is generated when the utilization matching a tmnxBsxStatTcaFtrEnCfgEntry in the past minute is greater than or equal to the value of tmnxBsxStatTcaFtrEnCfg HiWmark and the notification is not currently raised for the same entry. The tmnxBsxNotifyReason will identify the utilization.
Effect	There is no effect for this notification.

Property name	Value
Recovery	There is no recovery for this notification.

2.40 tmnxBsxStatFtrTcaThreshCrClear

Table 43: tmnxBsxStatFtrTcaThreshCrClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4454
Event name	tmnxBsxStatFtrTcaThreshCrClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.54
Default severity	minor
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$ $tmnxBsxNotifyTcaCfgFilterType$ " $tmnxBsxNotifyTcaCfgFilterName$" $tmnxBsxNotifyTcaCfgFltrWmarkType$* in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatFtrTcaThreshCrClear notification is generated when the utilization matching a tmnxBsxStatTcaFtrCfgEntry in the past minute is less than or equal to the value of tmnxBsxStatTcaFtrCfgLoWmark and tmnxBsxStatFtrTcaThreshCrossed is currently raised. The tmnxBsx NotifyReason will identify the utilization.
Effect	The tmnxBsxStatFtrTcaThreshCrossed notification is cleared.
Recovery	There is no recovery for this notification.

2.41 tmnxBsxStatFtrTcaThreshCrossed

Table 44: tmnxBsxStatFtrTcaThreshCrossed properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4453
Event name	tmnxBsxStatFtrTcaThreshCrossed
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.53

Property name	Value
Default severity	minor
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$ $tmnxBsxNotifyTcaCfgFilterType$* " *$tmnxBsxNotifyTcaCfgFilterName$*" *$tmnxBsxNotifyTcaCfgFltrWmarkType$* in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatFtrTcaThreshCrossed notification is generated when the utilization matching a tmnxBsxStatTcaFtrCfgEntry in the past minute is greater than or equal to the value of tmnxBsxStatTcaFtrCfgHiWmark and the notification is not currently raised for the same entry. The tmnx BsxNotifyReason will identify the utilization.
Effect	There is no effect for this notification.
Recovery	There is no recovery for this notification.

2.42 tmnxBsxStatPolcrTcaThreshCrClear

Table 45: tmnxBsxStatPolcrTcaThreshCrClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4452
Event name	tmnxBsxStatPolcrTcaThreshCrClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.52
Default severity	minor
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$* policer "*$tmnxBsxNotifyTcaPolicerName$*" in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatPolcrTcaThreshCrClear notification is generated when the utilization matching a tmnxBsxStatTcaPolcrCfgEntry in the past minute is less than or equal to the value of tmnxBsxStatTcaPolcrCfg LoWmark and tmnxBsxStatPolcrTcaThreshCrossed is currently raised. The tmnxBsxNotifyReason will identify the utilization.
Effect	The tmnxBsxStatPolcrTcaThreshCrossed notification is cleared.
Recovery	There is no recovery for this notification.

2.43 tmnxBsxStatPolcrTcaThreshCrossed

Table 46: tmnxBsxStatPolcrTcaThreshCrossed properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4451
Event name	tmnxBsxStatPolcrTcaThreshCrossed
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.51
Default severity	minor
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$* policer "*$tmnxBsxNotifyTcaPolicerName$*" in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatPolcrTcaThreshCrossed notification is generated when the utilization matching a tmnxBsxStatTcaPolcrCfgEntry in the past minute is greater than or equal to the value of tmnxBsxStatTcaPolcrCfgHiWmark and the notification is not currently raised for the same entry. The tmnxBsxNotifyReason will identify the utilization.
Effect	There is no effect for this notification.
Recovery	There is no recovery for this notification.

2.44 tmnxBsxStatTcaThreshCrossed

Table 47: tmnxBsxStatTcaThreshCrossed properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4449
Event name	tmnxBsxStatTcaThreshCrossed
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.49
Default severity	minor
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$ $tmnxBsxNotifyTcaCfgType$* in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatTcaThreshCrossed notification is generated when the utilization matching a tmnxBsxStatTcaCfgEntry in the past minute is

Property name	Value
	greater than or equal to the value of tmnxBsxStatTcaCfgHiWmark and the notification is not currently raised for the same entry. The tmnxBsx NotifyReason will identify the utilization.
Effect	There is no effect for this notification.
Recovery	There is no recovery for this notification.

2.45 tmnxBsxStatTcaThreshCrossedClear

Table 48: tmnxBsxStatTcaThreshCrossedClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4450
Event name	tmnxBsxStatTcaThreshCrossedClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.50
Default severity	minor
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotify AaGrpPartIndex$ $tmnxBsxNotifyTcaCfgType$* in the *$tmnxBsxNotify TcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxStatTcaThreshCrossedClear notification is generated when the utilization matching a tmnxBsxStatTcaCfgEntry in the past minute is less than or equal to the value of tmnxBsxStatTcaCfgLoWmark and tmnxBsxStatTcaThreshCrossed is currently raised. The tmnxBsxNotify Reason will identify the utilization.
Effect	The tmnxBsxStatTcaThreshCrossed notification is cleared.
Recovery	There is no recovery for this notification.

2.46 tmnxBsxSubModifyFailure

Table 49: tmnxBsxSubModifyFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4443

Property name	Value
Event name	tmnxBsxSubModifyFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.43
Default severity	minor
Message format string	Failed to *$tmnxBsxNotifySubFailedAction$* a subscriber in group *$tmnxBsxNotifyAaGrpPartIndex$* on ISA-MDA *$tmnxBsxNotifyActiveMda$* with reason: *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxSubModifyFailure notification is generated when a problem is encountered while attempting to apply an override (app-profile or ASO) to a subscriber based on information received from the Policy Server. The tmnxBsxNotifyReason will identify the reason this notification was raised.
Effect	The override is not applied to the subscriber.
Recovery	Based on the reason noted in tmnxBsxNotifyReason, if necessary take action to ensure that a configuration mismatch has not occurred to allow the overrides to be applied appropriately.

2.47 tmnxBsxTcpValTcaCrossed

Table 50: tmnxBsxTcpValTcaCrossed properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4460
Event name	tmnxBsxTcpValTcaCrossed
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.60
Default severity	minor
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$* TCP validate "*$tmnxBsxNotifyTcpValTcaName$*" in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxTcpValTcaCrossed notification is generated when the utilization matching a tmnxBsxTcpValTcaEntry in the past minute is greater than or equal to the value of tmnxBsxTcpValTcaHighWatermark and the notification is not currently raised for the same entry. The tmnxBsxNotifyReason will identify the utilization.

Property name	Value
Effect	There is no effect for this notification.
Recovery	There is no recovery for this notification.

2.48 tmnxBsxTcpValTcaCrossedClear

Table 51: tmnxBsxTcpValTcaCrossedClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4461
Event name	tmnxBsxTcpValTcaCrossedClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.61
Default severity	minor
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$* TCP validate "*$tmnxBsxNotifyTcpValTcaName$*" in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).
Cause	A tmnxBsxTcpValTcaCrossedClear notification is generated when the utilization matching a tmnxBsxTcpValTcaEntry in the past minute is less than or equal to the value of tmnxBsxTcpValTcaLowWatermark and tmnxBsxTcpValTcaCrossed is currently raised. The tmnxBsxNotifyReason will identify the utilization.
Effect	The tmnxBsxTcpValTcaCrossed notification is cleared.
Recovery	There is no recovery for this notification.

2.49 tmnxBsxTransIpPolAaSubCreated

Table 52: tmnxBsxTransIpPolAaSubCreated properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4421
Event name	tmnxBsxTransIpPolAaSubCreated

Property name	Value
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.21
Default severity	warning
Message format string	A dynamic transit subscriber *$tmnxBsxNotifyAaSubscriberName$* has been created in group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$*.
Cause	A tmnxBsxTransIpPolAaSubCreated notification is generated when a dynamic subscriber is created in a Transit IP Policy.
Effect	None.
Recovery	No recovery is required.

2.50 tmnxBsxTransIpPolAaSubDeleted

Table 53: tmnxBsxTransIpPolAaSubDeleted properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4422
Event name	tmnxBsxTransIpPolAaSubDeleted
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.22
Default severity	warning
Message format string	A dynamic transit subscriber *$tmnxBsxNotifyAaSubscriberName$* has been deleted from group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$*.
Cause	A tmnxBsxTransIpPolAaSubDeleted notification is generated when a dynamic subscriber is deleted in a Transit IP Policy.
Effect	None.
Recovery	No recovery is required.

2.51 tmnxBsxTransIpPolDhcpAddWarning

Table 54: tmnxBsxTransIpPolDhcpAddWarning properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4426
Event name	tmnxBsxTransIpPolDhcpAddWarning
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.26
Default severity	warning
Message format string	Problem encountered while attempting to add a transit subscriber to group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxTransIpPolDhcpAddWarning notification is generated when a problem occurs while attempting to add a dynamic transit subscriber learned via DHCP. The notification is informational and may not be an error. The tmnxBsxNotifyReason will identify the reason this trap was raised.
Effect	None.
Recovery	No recovery is required.

2.52 tmnxBsxTransIpPolDhcpDelWarning

Table 55: tmnxBsxTransIpPolDhcpDelWarning properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4427
Event name	tmnxBsxTransIpPolDhcpDelWarning
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.27
Default severity	warning
Message format string	Problem encountered while attempting to delete a transit subscriber from group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxTransIpPolDhcpDelWarning notification is generated when a problem occurs while attempting to delete a dynamic transit subscriber

Property name	Value
	learned via DHCP. The notification is informational and may not be an error. The tmnxBsxNotifyReason will identify the reason this trap was raised.
Effect	None.
Recovery	No recovery is required.

2.53 tmnxBsxTransIpPolDiamGxError

Table 56: tmnxBsxTransIpPolDiamGxError properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4457
Event name	tmnxBsxTransIpPolDiamGxError
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.57
Default severity	minor
Message format string	Problem encountered while processing a Diameter GX request/answer for group *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsx NotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxTransIpPolDiamGxError notification is generated when an error occurs while processing a Credit-Control Answer (CCA) or Re-Authorization Request (RAR) from a Diameter server over Gx. The tmnxBsxNotifyReason will identify the reason for failing to process the Diameter answer/request.
Effect	The addition or modification of a transit subscriber indicated in the Diameter Gx message will not have been performed.
Recovery	There is no recovery for this notification.

2.54 tmnxBsxTransIpPolRadCoAAudit

Table 57: tmnxBsxTransIpPolRadCoAAudit properties

Property name	Value
Application name	APPLICATION_ASSURANCE

Property name	Value
Event ID	4423
Event name	tmnxBsxTransIpPolRadCoAAudit
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.23
Default severity	warning
Message format string	CoA audit for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* is in state *$tmnxBsxNotifyRadiusCoAAuditState$*.
Cause	A tmnxBsxTransIpPolRadCoAAudit notification is generated when at the start and the end of the Change of Authorization (CoA) Audit.
Effect	None.
Recovery	No recovery is required.

2.55 tmnxBsxTransIpPolRadCoAError

Table 58: tmnxBsxTransIpPolRadCoAError properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4424
Event name	tmnxBsxTransIpPolRadCoAError
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.24
Default severity	minor
Message format string	Problem encountered while processing a CoA request for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$*: *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxTransIpPolRadCoAError notification is generated when an error occurs while processing a Change of Authorization (CoA) request from a RADIUS server. The tmnxBsxNotifyReason will identify the reason for failing to process the CoA request.
Effect	The addition or modification of a transit subscriber indicated in the CoA will not have been performed.
Recovery	No recovery is required.

2.56 tmnxBsxTransIpPolRadDiscError

Table 59: tmnxBsxTransIpPolRadDiscError properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4425
Event name	tmnxBsxTransIpPolRadDiscError
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.25
Default severity	minor
Message format string	Problem encountered while processing a RADIUS disconnect request for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.
Cause	A tmnxBsxTransIpPolRadDiscError notification is generated when an error occurs while processing a Disconect request from a RADIUS server. The tmnxBsxNotifyReason will identify the reason for failing to process the Disconnect request.
Effect	The removal of a transit subscriber indicated by a Disconnect request will not have been performed.
Recovery	No recovery is required.

2.57 tmnxBsxTransitIpPersistenceWarn

Table 60: tmnxBsxTransitIpPersistenceWarn properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4434
Event name	tmnxBsxTransitIpPersistenceWarn
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.34
Default severity	warning
Message format string	Problem encountered while registering transit subscriber address persistently for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.

Property name	Value
Cause	A tmnxBsxTransitIpPersistenceWarn notification is generated when a problem occurs while attempting to register a dynamic transit subscriber address with the persistence infrastructure. The tmnxBsx NotifyReason will identify the reason this trap was raised.
Effect	The affected transit subscriber address will not be persistent across a system reboot.
Recovery	No recovery is required.

2.58 tmnxBsxUrlFilterOperStateChange

Table 61: tmnxBsxUrlFilterOperStateChange properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4442
Event name	tmnxBsxUrlFilterOperStateChange
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.42
Default severity	warning
Message format string	AA Group *$tmnxBsxIsaAaGroupIndex$* URL Filter *$tmnxBsxUrlFilter Name$* state changed to *$tmnxBsxUrlFltrOperState$*, flags = *$tmnxBsx UrlFltrOperFlags$*.
Cause	The tmnxBsxUrlFilterOperStateChange notification is generated when the operational status of a URL Filter has transitioned either from 'in Service' to 'outOfService' or from 'outOfService' to 'inService'.
Effect	None.
Recovery	No recovery is required.

2.59 tmnxBsxUrlListFailure

Table 62: tmnxBsxUrlListFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4447

Property name	Value
Event name	tmnxBsxUrlListFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.47
Default severity	minor
Message format string	URL list "*$tmnxBsxUrlListName$*" in ISA-AA group *$tmnxBsxIsa AaGroupIndex$* has failed. The current operational state is: *$tmnxBsx UrlListStatusOperState$*, flags = *$tmnxBsxUrlListStatusOperFlags$*.
Cause	A tmnxBsxUrlListFailure notification is generated when a URL List has failed.
Effect	If the operational state is 'inService (2)', the URL List is operating using the last successfully processed list. If the operational state is 'out OfService (3)', there was no previous successful update and the URL List will be operationally down.
Recovery	The customer should ensure the correct file is configured in tmnxBsx UrlListFileUrl, and use tmnxBsxUrlListAdminState or tmnxBsxUrlList Upgrade to restart the URL List.

2.60 tmnxBsxUrlListUpdate

Table 63: tmnxBsxUrlListUpdate properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4446
Event name	tmnxBsxUrlListUpdate
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.46
Default severity	minor
Message format string	URL list "*$tmnxBsxUrlListName$*" in ISA-AA group *$tmnxBsxIsa AaGroupIndex$* has been updated. There are *$tmnxBsxUrlListStatus NumEntries$* entries in the URL list.
Cause	A tmnxBsxUrlListUpdate notification is generated when a URL List has been updated.
Effect	The URL List is installed on each ISA-AA in the group.
Recovery	There is no recovery for this notification.

3 APS

3.1 apsEventChannelMismatch

Table 64: apsEventChannelMismatch properties

Property name	Value
Application name	APS
Event ID	2003
Event name	apsEventChannelMismatch
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.3
Default severity	minor
Message format string	Channel Mismatch is declared
Cause	Channel Mismatch notification is generated due to mismatch between the transmitted K1 channel (phys port) and the received K2 channel (phys port).
Effect	N/A
Recovery	Configure both local and remote with the same channel type.

3.2 apsEventFEPLF

Table 65: apsEventFEPLF properties

Property name	Value
Application name	APS
Event ID	2005
Event name	apsEventFEPLF
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.5
Default severity	minor
Message format string	FEPL failure is declared

Property name	Value
Cause	FEPLF (Far-End Protection Line Failure) notification is generated based on SF (Signal Failure) condition on the protection port in the received K1 Byte.
Effect	Traffic will switch (Tx/Rx) to the working port if the traffic is presently Tx-ed/Rx-ed to/from the protection port.
Recovery	N/A

3.3 apsEventModeMismatch

Table 66: apsEventModeMismatch properties

Property name	Value
Application name	APS
Event ID	2002
Event name	apsEventModeMismatch
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.2
Default severity	minor
Message format string	Mode Mismatch is declared
Cause	Mode Mismatch notification is generated due to a conflict between the current local mode (switching direction or architecture) and the received K2 mode information.
Effect	For switching direction mismatch, the operational switching direction is changed to uni-directional. For switch architecture mismatch, the local end runs in 1+1 mode irrespective of the remote end switching architecture.
Recovery	Configure both local and remote end to run in same switching mode (direction/architecture).

3.4 apsEventPSBF

Table 67: apsEventPSBF properties

Property name	Value
Application name	APS

Property name	Value
Event ID	2004
Event name	apsEventPSBF
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.4
Default severity	minor
Message format string	PSB Failure is declared
Cause	A PSBF (Protection Switching Byte Failure) notification is generated due to inconsistent Rx K1 byte or invalid Rx K1 Byte.
Effect	A PSBF condition is considered as signal failure (SF) on the protection port.
Recovery	Correct the K1 byte value.

3.5 apsEventSwitchover

Table 68: apsEventSwitchover properties

Property name	Value
Application name	APS
Event ID	2001
Event name	apsEventSwitchover
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.1
Default severity	minor
Message format string	APS switchover from *$subject$*.
Cause	APS switchover between working port (channel 1) and protection port (channel 0) can happen due to change of status of any port or user initiated switch commands on any port.
Effect	Traffic is transmitted to and received from the other channel/port.
Recovery	None.

3.6 tApsChannelMismatchClear

Table 69: tApsChannelMismatchClear properties

Property name	Value
Application name	APS
Event ID	2007
Event name	tApsChannelMismatchClear
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.2
Default severity	minor
Message format string	Channel Mismatch is cleared
Cause	The Channel mismatch clear notification is generated when the current status of an APS group gets the channel mismatch condition cleared.
Effect	N/A
Recovery	N/A

3.7 tApsChanTxLaisStateChange

Table 70: tApsChanTxLaisStateChange properties

Property name	Value
Application name	APS
Event ID	2015
Event name	tApsChanTxLaisStateChange
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.10
Default severity	warning
Message format string	APS forced Tx-LAIS state changed to *$tApsChanTxLaisState$*
Cause	The tApsChanTxLaisStateChange notification is generated when there is a change in the value of tApsChanTxLaisState.
Effect	N/A
Recovery	Investigation is required to determine the cause of the change.

3.8 tApsFEPLFClear

Table 71: tApsFEPLFClear properties

Property name	Value
Application name	APS
Event ID	2009
Event name	tApsFEPLFClear
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.4
Default severity	minor
Message format string	FEPL Failure is cleared
Cause	The FEPLF clear notification is generated when the current status of an APS group gets the FEPLF condition cleared.
Effect	N/A
Recovery	N/A

3.9 tApsLocalSwitchCommandClear

Table 72: tApsLocalSwitchCommandClear properties

Property name	Value
Application name	APS
Event ID	2011
Event name	tApsLocalSwitchCommandClear
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.6
Default severity	warning
Message format string	Local - *$apsCommandSwitch$* cleared
Cause	The tApsLocalSwitchCommandClear notification is generated when an APS switch command in the local node gets cleared. Note that a switch command in the local node can be cleared either due to execution of the clear switch command in the local node or due to presence of a higher priority condition in the local or remote node.
Effect	N/A
Recovery	N/A

3.10 tApsLocalSwitchCommandSet

Table 73: tApsLocalSwitchCommandSet properties

Property name	Value
Application name	APS
Event ID	2010
Event name	tApsLocalSwitchCommandSet
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.5
Default severity	warning
Message format string	Local - *$apsCommandSwitch$* set
Cause	The tApsLocalSwitchCommandSet is generated when any of the following APS switch commands is executed on an APS channel in the local node. The switch commands are lockoutOfProtection, forced SwitchWorkToProtect, forcedSwitchProtectToWork, manualSwitchWork ToProtect, and manualSwitchProtectToWork.
Effect	N/A
Recovery	N/A

3.11 tApsMcApsCtlLinkStateChange

Table 74: tApsMcApsCtlLinkStateChange properties

Property name	Value
Application name	APS
Event ID	2014
Event name	tApsMcApsCtlLinkStateChange
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.9
Default severity	warning
Message format string	Control link state changed to *$tApsMcApsCtlLinkState$*
Cause	The tApsMcApsCtlLinkStateChange notification is generated when there is a change in the value of tApsMcApsCtlLinkState.
Effect	N/A

Property name	Value
Recovery	Investigation is required to determine the cause of the change.

3.12 tApsModeMismatchClear

Table 75: tApsModeMismatchClear properties

Property name	Value
Application name	APS
Event ID	2006
Event name	tApsModeMismatchClear
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.1
Default severity	minor
Message format string	Mode Mismatch is cleared
Cause	The Mode mismatch clear notification is generated when the current status of an APS group gets the mode mismatch condition cleared.
Effect	N/A
Recovery	N/A

3.13 tApsPrimaryChannelChange

Table 76: tApsPrimaryChannelChange properties

Property name	Value
Application name	APS
Event ID	2016
Event name	tApsPrimaryChannelChange
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.11
Default severity	minor
Message format string	Switch of the primary APS channel to *$apsStatusK1K2Trans$*.

Property name	Value
Cause	The tApsPrimaryChannelChange notification is generated when there is a switch of the primary APS channel. Object apsStatusK1K2Trans indicates the new primary APS channel.
Effect	N/A
Recovery	Investigation is required to determine the cause of the change.

3.14 tApsPSBFClear

Table 77: tApsPSBFClear properties

Property name	Value
Application name	APS
Event ID	2008
Event name	tApsPSBFClear
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.3
Default severity	minor
Message format string	PSB Failure is cleared
Cause	The PSBF clear notification is generated when the current status of an APS group gets the PSBF condition cleared.
Effect	N/A
Recovery	N/A

3.15 tApsRemoteSwitchCommandClear

Table 78: tApsRemoteSwitchCommandClear properties

Property name	Value
Application name	APS
Event ID	2013
Event name	tApsRemoteSwitchCommandClear
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.8

Property name	Value
Default severity	warning
Message format string	Remote - *$apsCommandSwitch$* cleared
Cause	The tApsRemoteSwitchCommandClear is generated when the received K1 byte (APS-MIB::apsStatusK1K2Rcv) from a peer indicates that an APS switch command just got cleared on an APS channel in the remote (peer) node.
Effect	N/A
Recovery	N/A

3.16 tApsRemoteSwitchCommandSet

Table 79: tApsRemoteSwitchCommandSet properties

Property name	Value
Application name	APS
Event ID	2012
Event name	tApsRemoteSwitchCommandSet
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.7
Default severity	warning
Message format string	Remote - *$apsCommandSwitch$* set
Cause	The tApsRemoteSwitchCommandSet is generated when the received K1 byte (APS-MIB::apsStatusK1K2Rcv) from a peer indicates that an APS switch command just got executed on an APS channel in the remote (peer) node.
Effect	N/A
Recovery	Investigation is required to determine the cause of the change.

4 ATM

4.1 atmIfcStatusChange

Table 80: atmIfcStatusChange properties

Property name	Value
Application name	ATM
Event ID	2009
Event name	atmIfcStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Status of *$subject$* owned by *$tAtmIfcInfoOwner$* has changed to administrative state: *$tAtmIfcAdminStatus$* operational state: *$tAtmIfc OperStatus$*
Cause	The state of the ATM interface has changed.
Effect	N/A
Recovery	N/A

4.2 atmIlmiPeerVclStatusChange

Table 81: atmIlmiPeerVclStatusChange properties

Property name	Value
Application name	ATM
Event ID	2016
Event name	atmIlmiPeerVclStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Status of VCL *$atmVclVpi$*/*$atmVclVci$* on *$subject$* has changed to operational state: *$atmVclOperStatus$*

Property name	Value
Cause	The state of the ILMI peer VCL has changed.
Effect	N/A
Recovery	Investigate what caused the new state.

4.3 atmIlmiPeerVplStatusChange

Table 82: atmIlmiPeerVplStatusChange properties

Property name	Value
Application name	ATM
Event ID	2017
Event name	atmIlmiPeerVplStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Status of VPL *$atmVplVpi$* on *$subject$* has changed to operational state: *$atmVplOperStatus$*
Cause	The state of the ILMI peer VPL has changed.
Effect	N/A
Recovery	Investigate what caused the new state.

4.4 atmVclStatusChange

Table 83: atmVclStatusChange properties

Property name	Value
Application name	ATM
Event ID	2006
Event name	atmVclStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning

Property name	Value
Message format string	Status of *$subject$* owned by *$tAtmVclInfoOwner$* has changed to administrative state: *$atmVclAdminStatus$* operational state: *$atmVcl OperStatus$* OAM state: *$tAtmVclInfoOamStatus$*
Cause	The state of the ATM VCL has changed.
Effect	N/A
Recovery	N/A

4.5 atmVplStatusChange

Table 84: atmVplStatusChange properties

Property name	Value
Application name	ATM
Event ID	2007
Event name	atmVplStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Status of *$subject$* owned by *$tAtmVplInfoOwner$* has changed to administrative state: *$atmVplAdminStatus$* operational state: *$atmVpl OperStatus$* OAM state: *$tAtmVplInfoOamStatus$*
Cause	The state of the ATM VPL has changed.
Effect	N/A
Recovery	N/A

4.6 atmVtlStatusChange

Table 85: atmVtlStatusChange properties

Property name	Value
Application name	ATM
Event ID	2008
Event name	atmVtlStatusChange

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Status of *$subject$* owned by *$tAtmVtlInfoOwner$* has changed to administrative state: *$tAtmVtlAdminStatus$* operational state: *$tAtmVtl OperStatus$*
Cause	The state of the ATM VTL has changed.
Effect	N/A
Recovery	N/A

4.7 tAtmEpOutOfPeerVpiOrVciRange

Table 86: tAtmEpOutOfPeerVpiOrVciRange properties

Property name	Value
Application name	ATM
Event ID	2012
Event name	tAtmEpOutOfPeerVpiOrVciRange
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.5
Default severity	warning
Message format string	ATM EPs on ATM interface *$subject$* are outside of the negotiated VPI or VCI range
Cause	The tAtmEpOutOfPeerVpiOrVciRange notification is sent whenever an ILMI link becomes operationally up and ATM EPs are configured on the ILMI-managed interface that are outside the VPI or VCI range allowed by the peer.
Effect	N/A
Recovery	Adjust the VPI or VCI range.

4.8 tAtmIlmiLinkStatusChange

Table 87: tAtmIlmiLinkStatusChange properties

Property name	Value
Application name	ATM
Event ID	2015
Event name	tAtmIlmiLinkStatusChange
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.8
Default severity	warning
Message format string	Status of ILMI on ATM Interface *$subject$* vpi=*$tAtmIlmiLinkVpi$* vci=*$tAtmIlmiLinkVci$* has changed administrative status: *$tAtmIlmiLinkAdminStatus$* operational status: *$tAtmIlmiLinkOperStatus$*
Cause	The tAtmIlmiLinkStatusChange notification is sent whenever a status change occurs on an ILMI link. This includes changes to the ILMI link's administrative status and the ILMI link's operational status.
Effect	N/A
Recovery	N/A

4.9 tAtmMaxPeerVccsExceeded

Table 88: tAtmMaxPeerVccsExceeded properties

Property name	Value
Application name	ATM
Event ID	2013
Event name	tAtmMaxPeerVccsExceeded
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.6
Default severity	warning
Message format string	The number of ATM VCLs on ATM interface *$subject$* exceeds the negotiated maximum
Cause	The tAtmMaxPeerVccsExceeded notification is sent whenever an ILMI link becomes operationally up and there are more ATM VCLs configured on the ILMI-managed interface than are supported by the peer.

Property name	Value
Effect	N/A
Recovery	N/A

4.10 tAtmMaxPeerVpcsExceeded

Table 89: tAtmMaxPeerVpcsExceeded properties

Property name	Value
Application name	ATM
Event ID	2014
Event name	tAtmMaxPeerVpcsExceeded
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.7
Default severity	warning
Message format string	The number of ATM VPLs on ATM interface *$subject$* exceeds the negotiated maximum
Cause	The tAtmMaxPeerVpcsExceeded notification is sent whenever an ILMI link becomes operationally up and there are more ATM VPLs configured on the ILMI-managed interface than are supported by the peer.
Effect	N/A
Recovery	N/A

4.11 tAtmPlcpSubLayerClear

Table 90: tAtmPlcpSubLayerClear properties

Property name	Value
Application name	ATM
Event ID	2011
Event name	tAtmPlcpSubLayerClear
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.4
Default severity	minor

Property name	Value
Message format string	ATM Interface *$subject$* entered the no error state
Cause	The tAtmPlcpSubLayerClear notification is generated when the ATM interface has left the far end alarm or incoming LOF error state and entered the no error state.
Effect	N/A
Recovery	N/A

4.12 tAtmPlcpSubLayerDown

Table 91: tAtmPlcpSubLayerDown properties

Property name	Value
Application name	ATM
Event ID	2010
Event name	tAtmPlcpSubLayerDown
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.3
Default severity	minor
Message format string	ATM Interface *$subject$* entered failure state
Cause	The tAtmPlcpSubLaerDown notification is generated when the ATM interface has left the no error state and entered the far end alarm or incoming LOF state.
Effect	N/A
Recovery	N/A

4.13 tAtmTcSubLayerClear

Table 92: tAtmTcSubLayerClear properties

Property name	Value
Application name	ATM
Event ID	2005
Event name	tAtmTcSubLayerClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.2
Default severity	minor
Message format string	ATM Interface *$subject$* entered the LCD no error state
Cause	The tAtmTcSubLayerClear notification is generated when the ATM interface has left the Loss of Cell Delineation (LCD) error state and entered the LCD no error state.
Effect	N/A
Recovery	N/A

4.14 tAtmTcSubLayerDown

Table 93: tAtmTcSubLayerDown properties

Property name	Value
Application name	ATM
Event ID	2004
Event name	tAtmTcSubLayerDown
SNMP notification prefix and OID	TIMETRA-ATM-MIB.tAtmNotifications.1
Default severity	minor
Message format string	ATM Interface *$subject$* entered LCD failure state
Cause	The tAtmTcSubLayerUp notification is generated when the ATM interface has left the no error Loss of Cell Delineation (LCD) state and entered the default LCD state.
Effect	N/A
Recovery	Investigate why the ATM TC Sublayer is currently in the LCD state.

5 BFD

5.1 tmnxBfdOnLspSessDeleted

Table 94: tmnxBfdOnLspSessDeleted properties

Property name	Value
Application name	BFD
Event ID	2003
Event name	tmnxBfdOnLspSessDeleted
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.3
Default severity	minor
Message format string	The *$tmnxBfdOnLspSessLinkType$* BFD Session with Local Discriminator *$tmnxBfdOnLspSessLclDisc$* on *$subject$* has been deleted
Cause	The tmnxBfdOnLspSessDeleted notification is generated when a BFD on LSP session is deleted.
Effect	The deletion of this session will either take down any protocol that is riding over top of it or notifies them that the session has been deleted.
Recovery	There is no recovery required for this notification.

5.2 tmnxBfdOnLspSessDown

Table 95: tmnxBfdOnLspSessDown properties

Property name	Value
Application name	BFD
Event ID	2001
Event name	tmnxBfdOnLspSessDown
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.1
Default severity	minor

Property name	Value
Message format string	The *$tmnxBfdOnLspSessLinkType$* BFD session with Local Discriminator *$tmnxBfdOnLspSessLclDisc$* on *$subject$* is down due to *$tmnxBfdOnLspSessOperFlags$*
Cause	The tmnxBfdOnLspSessDown notification is generated when a BFD on LSP session goes down.
Effect	The effect of this session going down is that it either takes down any protocol that is riding over top of it or it notifies them that the session has gone down.
Recovery	The session will automatically attempt to re-establish on it's own.

5.3 tmnxBfdOnLspSessNoCpmNpResources

Table 96: tmnxBfdOnLspSessNoCpmNpResources properties

Property name	Value
Application name	BFD
Event ID	2005
Event name	tmnxBfdOnLspSessNoCpmNpResources
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.5
Default severity	minor
Message format string	The *$tmnxBfdOnLspSessLinkType$* BFD session with local discriminator *$tmnxBfdOnLspSessLclDisc$* on *$subject$* could not be established because cpm-np session termination resources are not available
Cause	The tmnxBfdOnLspSessNoCpmNpResources notification is generated when a BFD on LSP session could not be established because the session requires a cpmNp session termination resource (see TIMETRA-VRTR-MIB::vRtrIfBfdExtType), and no cpmNp session termination resources are available.
Effect	The BFD session cannot be established until a cpmNp session termination resource is available
Recovery	There is no recovery required for this notification.

5.4 tmnxBfdOnLspSessProtChange

Table 97: tmnxBfdOnLspSessProtChange properties

Property name	Value
Application name	BFD
Event ID	2004
Event name	tmnxBfdOnLspSessProtChange
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.4
Default severity	minor
Message format string	The protocol (*$tmnxBfdOnLspSessChangedProtocol$*) using BFD session on node *$subject$* has been *$tmnxBfdOnLspSessProtoChngd State$*
Cause	The tmnxBfdOnLspSessProtChange notification is generated when there is a change in the list of protocols specified by tmnxBfdOnLsp SessProtocols using the BFD on LSP session.
Effect	The list of protocols using this session are modified.
Recovery	There is no recovery required for this notification.

5.5 tmnxBfdOnLspSessUp

Table 98: tmnxBfdOnLspSessUp properties

Property name	Value
Application name	BFD
Event ID	2002
Event name	tmnxBfdOnLspSessUp
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.2
Default severity	minor
Message format string	The *$tmnxBfdOnLspSessLinkType$* BFD session with Local Discriminator *$tmnxBfdOnLspSessLclDisc$* on *$subject$* is up
Cause	The tmnxBfdOnLspSessUp notification is generated when a BFD on LSP session goes up.
Effect	The BFD session will be active.

Property name	Value
Recovery	There is no recovery required for this notification.

6 BGP

6.1 bgpBackwardTransNotification

Table 99: bgpBackwardTransNotification properties

Property name	Value
Application name	BGP
Event ID	2039
Event name	bgpBackwardTransNotification
SNMP notification prefix and OID	BGP4-MIB.bgpNotification.2
Default severity	warning
Message format string	*bgp_peer_name*: moved from higher state *old_state_str* to lower state *new_state_str* due to event *$event_str$*
Cause	The bgpBackwardTransNotification event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. This Notification replaces the bgpBackwardsTransition Notification.
Effect	N/A
Recovery	N/A

6.2 bgpCfgViol

Table 100: bgpCfgViol properties

Property name	Value
Application name	BGP
Event ID	2017
Event name	bgpCfgViol
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*$subject$*: BGP - *$field$* configuration ignored - *$reason$*

Property name	Value
Cause	BGP configuration was invalid.
Effect	The configuration that lead to the violation will be totally ignored.
Recovery	N/A

6.3 bgpConnMgrTerminated

Table 101: bgpConnMgrTerminated properties

Property name	Value
Application name	BGP
Event ID	2013
Event name	bgpConnMgrTerminated
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*$subject$*: BGP connection manager for address family *$addr_family_str$* has terminated
Cause	BGP is being shutdown or deleted.
Effect	No inbound BGP connections will be accepted.
Recovery	BGP must be re-enabled.

6.4 bgpConnNoKA

Table 102: bgpConnNoKA properties

Property name	Value
Application name	BGP
Event ID	2008
Event name	bgpConnNoKA
SNMP notification prefix and OID	N/A
Default severity	warning

Property name	Value
Message format string	*bgp_peer_name*: closing inbound connection because the BGP peer did not receive "keepalive"
Cause	A BGP KEEPALIVE message was not recieved within the holdtime limit.
Effect	Inbound connection failed to establish.
Recovery	Reset and try again.

6.5 bgpConnNoOpenRcvd

Table 103: bgpConnNoOpenRcvd properties

Property name	Value
Application name	BGP
Event ID	2009
Event name	bgpConnNoOpenRcvd
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: closing inbound connection because the BGP peer did not receive "open"
Cause	A BGP OPEN message was not recieved within the holdtime limit.
Effect	Inbound connection failed to establish.
Recovery	Reset and try again.

6.6 bgpEstablishedNotification

Table 104: bgpEstablishedNotification properties

Property name	Value
Application name	BGP
Event ID	2038
Event name	bgpEstablishedNotification

Property name	Value
SNMP notification prefix and OID	BGP4-MIB.bgpNotification.1
Default severity	minor
Message format string	*bgp_peer_name*: moved into established state
Cause	The bgpEstablishedNotification event is generated when the BGP FSM enters the established state. This Notification replaces the bgp Established Notification.
Effect	The BGP instance is now running.
Recovery	N/A

6.7 bgpInterfaceDown

Table 105: bgpInterfaceDown properties

Property name	Value
Application name	BGP
Event ID	2007
Event name	bgpInterfaceDown
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: being disabled because the interface is operationally disabled
Cause	The IP interface is down.
Effect	All EBGP peers directly attached to the interface for the peering go down.
Recovery	Bring the interface up.

6.8 bgpNoMemoryPeer

Table 106: bgpNoMemoryPeer properties

Property name	Value
Application name	BGP

Property name	Value
Event ID	2015
Event name	bgpNoMemoryPeer
SNMP notification prefix and OID	N/A
Default severity	critical
Message format string	*bgp_peer_name*: out of memory - disabled the peer
Cause	The router has run out of memory.
Effect	The peering that first hit the out of memory condition on a memory allocation request is going to go down and it will be marked DISABLED.
Recovery	Upgrade the box's memory or shut down the memory hogging peering sessions.

6.9 bgpPeerNotFound

Table 107: bgpPeerNotFound properties

Property name	Value
Application name	BGP
Event ID	2012
Event name	bgpPeerNotFound
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*$subject$*: Closing connection: *$peer_ip_str$* not enabled or not in configuration
Cause	BGP peering session won't come up.
Effect	Inbound connection failed to establish as the peer that the remote end is trying to connect to does not exist in the current configuration.
Recovery	Change the BGP configuration to create a peering session with the remote peer.

6.10 bgpRejectConnBadLocAddr

Table 108: bgpRejectConnBadLocAddr properties

Property name	Value
Application name	BGP
Event ID	2010
Event name	bgpRejectConnBadLocAddr
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: inbound connection rejected because the BGP peer received connection attempt on *rcv_addr_str* but it only accepts connection on *lcl_addr_str*
Cause	Inbound BGP connection not being attempted through the correct IP address.
Effect	Inbound connection will be rejected - failed to establish the peering session.
Recovery	The remote peer should be trying to open the peering connection to the appropriate IP address - i.e. the one mentioned in the local-address of the local peer.

6.11 bgpRemoteEndClosedConn

Table 109: bgpRemoteEndClosedConn properties

Property name	Value
Application name	BGP
Event ID	2011
Event name	bgpRemoteEndClosedConn
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: remote end closed connection
Cause	The remote end of the BGP connection closed the TCP connection.
Effect	The BGP peering session is closed. All routes learnt from that peer were rejected.

Property name	Value
Recovery	Reset and try to re-establish the peering.

6.12 bgpTerminated

Table 110: bgpTerminated properties

Property name	Value
Application name	BGP
Event ID	2014
Event name	bgpTerminated
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*$subject$*: BGP has terminated
Cause	BGP is being shutdown or deleted.
Effect	The BGP protocol will terminate.
Recovery	BGP must be re-enabled.

6.13 bgpVariableRangeViolation

Table 111: bgpVariableRangeViolation properties

Property name	Value
Application name	BGP
Event ID	2016
Event name	bgpVariableRangeViolation
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*$subject$*: trying to set *$varname$* to *$tryval$* - valid range is [*$minval $-$maxval$*] - setting to *$finalval$*
Cause	The event is caused by setting some variable through a MIB that is outside the valid range accepted by the application. The system gets into this scenario when the agent is not able to catch the variable

Property name	Value
	range violation because from the perspective of the MIB variable that is being set it is an acceptable value. e.g. min-route-advertisement has a range in the Nokia MIB that is more strict than the standard BGP4 MIB. Although the agent will allow larger range values for this MIB variable the BGP implementation will reject it as it is restricted by the the Nokia BGP MIB.
Effect	The set value is not accepted but the closest valid value to the set value is accepted.
Recovery	N/A

6.14 receiveNotification

Table 112: receiveNotification properties

Property name	Value
Application name	BGP
Event ID	2006
Event name	receiveNotification
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: received notification: code *$code_str$* subcode *$subcode_str$*
Cause	Any error that occured between BGP peers that was first recognized by the remote BGP instance. e.g. 1) An error occured in the state transitions of a peering session. 2) An error occured during the exchange of routing information between BGP peers. 3) The two BGP peers mismatch on the capability that they can support.
Effect	The system closes the existing socket connection and tries to establish the peering session again.
Recovery	N/A

6.15 sendNotification

Table 113: sendNotification properties

Property name	Value
Application name	BGP
Event ID	2005
Event name	sendNotification
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: sending notification: code *$code_str$* subcode *$subcode_str$*
Cause	Any error that occured between BGP peers that was first recognized by the local BGP instance. e.g. 1) An error occured in the state transitions of a peering session. 2) An error occured during the exchange of routing information between BGP peers. 3) The two BGP peers mismatch on the capability that they can support.
Effect	The system brings down the peering and attempts to establish a new peering session.
Recovery	N/A

6.16 tBgp4PathAttrInvalid

Table 114: tBgp4PathAttrInvalid properties

Property name	Value
Application name	BGP
Event ID	2028
Event name	tBgp4PathAttrInvalid
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.16
Default severity	warning
Message format string	*$vRtrID$*: BGP Peer *$tBgpPeerNgAddr$*: Invalid path attribute received with attribute type [*$tBgp4PathAttrType$*] and length [*$tBgp4PathAttr Length$*]. Hex dump: *$tBgp4PathAttribute$*

Property name	Value
Cause	The tBgp4PathAttrInvalid notification is generated when an error with a path attribute tBgp4PathAttribute is detected.
Effect	A log entry is generated for each withdrawn route. Further effect depends on fault-tolerance and graceful-restart settings.
Recovery	There is no recovery required for this notification.

6.17 tBgp4RouteInvalid

Table 115: tBgp4RouteInvalid properties

Property name	Value
Application name	BGP
Event ID	2027
Event name	tBgp4RouteInvalid
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.15
Default severity	warning
Message format string	*$vRtrID$*: BGP Peer: *$tBgpPeerNgAddr$*, Route invalid Reason - *$tBgpRouteInvalidReason$* NLRI - *$tBgpRouteNLRI$*
Cause	The tBgp4RouteInvalid notification is generated when the received route is invalid for a specific reason and the route can not be used or advertised further.
Effect	The BGP peer ignores the route and flags the path attribute and the route so that the peer/tribe that was attempting to advertise the associated route can skip this route. The BGP peering is not torn down in this case.
Recovery	There is no recovery required for this notification.

6.18 tBgp4UpdateInvalid

Table 116: tBgp4UpdateInvalid properties

Property name	Value
Application name	BGP

Property name	Value
Event ID	2030
Event name	tBgp4UpdateInvalid
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.18
Default severity	warning
Message format string	*$vRtrID$*: BGP Peer: *$tBgpPeerNgAddr$*. Hex dump: *$tBgp4UpdateMessage$*
Cause	The tBgp4UpdateInvalid notification is generated when an UPDATE message has a critical length error or an error not specific to any path attribute.
Effect	A log entry is generated for each withdrawn route. Further effect depends on fault-tolerance and graceful-restart settings.
Recovery	There is no recovery required for this notification.

6.19 tBgp4WithdrawnRtFromUpdateError

Table 117: tBgp4WithdrawnRtFromUpdateError properties

Property name	Value
Application name	BGP
Event ID	2029
Event name	tBgp4WithdrawnRtFromUpdateError
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.17
Default severity	warning
Message format string	*$vRtrID$*: BGP Peer: *$tBgpPeerNgAddr$*, Route: *$tBgp4WithdrawnRoutePrefix$* withdrawn because of error in BGP update message.
Cause	The tBgp4WithdrawnRtFromUpdateError notification is generated when NLRI is withdrawn because of error in BGP update message.
Effect	This notification has no direct effect. The withdrawn routes are logged to aid debugging and tracking back the root cause of the problem.
Recovery	There is no recovery required for this notification.

6.20 tBgpFibResourceFailPeer

Table 118: tBgpFibResourceFailPeer properties

Property name	Value
Application name	BGP
Event ID	2032
Event name	tBgpFibResourceFailPeer
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	*bgp_peer_name*: FIB resource fail - disabled the peer
Cause	The router has run out of memory. It is triggered when BGP fails to add a route into RTM.
Effect	The system disables the peer.
Recovery	There is no automatic recovery. The user has to manually enable the peer again.

6.21 tBgpFlowRouteInvalid

Table 119: tBgpFlowRouteInvalid properties

Property name	Value
Application name	BGP
Event ID	2023
Event name	tBgpFlowRouteInvalid
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.11
Default severity	warning
Message format string	*bgp_peer_name*: Invalid flow route received from peer [*$tBgpPeer NgAddr$*] for destination [*$tBgpPeerFlowRouteDestAddr$*] Reason - [*$tBgpFlowRouteInvalidReason$*] NLRI - [*$tBgpFlowRouteNLRI$*].
Cause	The tBgpFlowRouteInvalid notification is generated when the received BGP flow route is invalid.
Effect	The BGP peer does not create ip filter entry for the received flow route.

Property name	Value
Recovery	There is no recovery required for this notification.

6.22 tBgpFlowspecUnsupportdComAction

Table 120: tBgpFlowspecUnsupportdComAction properties

Property name	Value
Application name	BGP
Event ID	2022
Event name	tBgpFlowspecUnsupportdComAction
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.10
Default severity	warning
Message format string	*bgp_peer_name*: Flowspec NLRI - unsupported community action : [*$tBgpFlowspecExtCommunityAction$*], action value : [*$tBgpFlowspecExtCommActionValue$*] received.
Cause	The tBgpFlowspecUnsupportdComAction notification is generated when the best route for a flow specification NLRI(Network Layer Reachability Information) is received from a remote BGP peer with an extended community action that is unsupported.
Effect	The BGP peer dose not create ip filter entry for the received flow route even if the NLRI(Network Layer Reachability Information) has valid extended community actions.
Recovery	There is no recovery required for this notification.

6.23 tBgpGeneral

Table 121: tBgpGeneral properties

Property name	Value
Application name	BGP
Event ID	2031
Event name	tBgpGeneral
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	warning
Message format string	*$subject$*: *$title$* *$message$*
Cause	The general event is generated when certain error conditions are reported by the BGP application.
Effect	Each condition has its own effect.
Recovery	The recovery depends on the condition reported.

6.24 tBgpInstanceDynamicPeerLmtReachd

Table 122: tBgpInstanceDynamicPeerLmtReachd properties

Property name	Value
Application name	BGP
Event ID	2036
Event name	tBgpInstanceDynamicPeerLmtReachd
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.22
Default severity	minor
Message format string	*bgp_peer_name*: Closing connection: reached dynamic peer limit (*$tBgpInstanceDynamicPeerLimit$*) for BGP instance *$tBgpInstanceIndex$*
Cause	A tBgpInstanceDynamicPeerLmtReachd notification is generated when the dynamic peer limit for this BGP instance is reached.
Effect	Whenever an incoming connection for a new dynamic session would cause dynamic peer limit for this BGP instance to be exceeded, the connection attempt is rejected.
Recovery	Increase the dynamic peer limit for this BGP instance.

6.25 tBgpMaxNgPfxLmt

Table 123: tBgpMaxNgPfxLmt properties

Property name	Value
Application name	BGP
Event ID	2034
Event name	tBgpMaxNgPfxLmt
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.20
Default severity	minor
Message format string	*bgp_peer_name*: number of routes learned has exceeded configured maximum (*$tBgpPeerNgPfxLmtMaxPrefix$*) for *$tBgpPeerNgPfxLmt Family$* family
Cause	A tBgpMaxNgPfxLmt notification is generated when the number of routes learned from the peer has exceeded the configured maximum.
Effect	No direct effect but if the peer continues to advertise more routes then the number of routes may exceed the configured maximum (tBgpPeer NgPfxLmtMaxPrefix). In that case the peer would just be disabled.
Recovery	Increase the max-prefix for this peer.

6.26 tBgpMaxNgPfxLmtThresholdReached

Table 124: tBgpMaxNgPfxLmtThresholdReached properties

Property name	Value
Application name	BGP
Event ID	2035
Event name	tBgpMaxNgPfxLmtThresholdReached
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.21
Default severity	minor
Message format string	*bgp_peer_name*: number of routes learned has exceeded *$tBgpPeer NgPfxLmtThreshold$* percentage of the configured maximum (*$tBgp PeerNgPfxLmtMaxPrefix$*) for *$tBgpPeerNgPfxLmtFamily$* family
Cause	A tBgpMaxNgPfxLmtThresholdReached notification is generated when the number of routes learned from the peer has exceeded tBgpPeer

Property name	Value
	NgPfxLmtThreshold percent of the configured maximum (tBgpPeer NgPfxLmtMaxPrefix).
Effect	No direct effect but if the peer continues to advertise more routes then the number of routes may exceed the configured maximum (tBgpPeer NgPfxLmtMaxPrefix). In that case the peer would just be disabled.
Recovery	Increase the max-prefix for this peer.

6.27 tBgpNgBackwardTransition

Table 125: tBgpNgBackwardTransition properties

Property name	Value
Application name	BGP
Event ID	2020
Event name	tBgpNgBackwardTransition
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.8
Default severity	warning
Message format string	*bgp_peer_name*: moved from higher state *old_state_str* to lower state *new_state_str* due to event *$event_str$*
Cause	The tBgpNgBackwardTransition notification is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.
Effect	N/A
Recovery	N/A

6.28 tBgpNgEstablished

Table 126: tBgpNgEstablished properties

Property name	Value
Application name	BGP
Event ID	2019
Event name	tBgpNgEstablished

Property name	Value
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.7
Default severity	minor
Message format string	*bgp_peer_name*: moved into established state
Cause	The tBgpNgEstablished notification is generated when the BGP FSM enters the ESTABLISHED state.
Effect	The BGP instance is now running.
Recovery	N/A

6.29 tBgpPeerGRStatusChange

Table 127: tBgpPeerGRStatusChange properties

Property name	Value
Application name	BGP
Event ID	2018
Event name	tBgpPeerGRStatusChange
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.6
Default severity	warning
Message format string	*bgp_peer_name*: graceful restart status changed to *$tBgpPeer NgOperGRStatus$*
Cause	The BGP peer is either restarting or just changed the graceful restart status to 'helping'/'not helping'/'restart complete'.
Effect	N/A
Recovery	N/A

6.30 tBgpPeerNgHoldTimeInconsistent

Table 128: tBgpPeerNgHoldTimeInconsistent properties

Property name	Value
Application name	BGP

Property name	Value
Event ID	2021
Event name	tBgpPeerNgHoldTimeInconsistent
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.9
Default severity	warning
Message format string	*bgp_peer_name*: attempted to negotiate a hold timer lower than the configured minimum value of *$tBgpPeerNgMinHoldTime$*
Cause	The BGP peer tried to establish a peering with a hold time less than the configured minimum hold time value.
Effect	The BGP peering is rejected.
Recovery	Establish peering with a hold time equal to or greater than the minimum hold time configured.

6.31 tBgpPGDynamicPeerLmtReached

Table 129: tBgpPGDynamicPeerLmtReached properties

Property name	Value
Application name	BGP
Event ID	2037
Event name	tBgpPGDynamicPeerLmtReached
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.23
Default severity	minor
Message format string	*bgp_peer_name*: Closing connection: reached dynamic peer limit (*$tBgpPGDynamicPeerLimit$*) for BGP group *$tBgpPeerGroupName$*
Cause	A tBgpPGDynamicPeerLmtReached notification is generated when when the dynamic peer limit for this group is reached.
Effect	Whenever an incoming connection for a new dynamic session would cause dynamic peer limit for this group to be exceeded, the connection attempt is rejected.
Recovery	Increase the dynamic peer limit for this group.

6.32 tBgpReceivedInvalidNlri

Table 130: tBgpReceivedInvalidNlri properties

Property name	Value
Application name	BGP
Event ID	2033
Event name	tBgpReceivedInvalidNlri
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.19
Default severity	warning
Message format string	For the bad_network error type *$tBgp4BadErrorMessageType$* the message received is *$tBgp4BadErrorMessage$*.
Cause	The tBgpReceivedInvalidNlri notification is generated when there is a parsing error in BGP routes that is not related to attribute errors.
Effect	BGP will send a notification message to the peer and bring down the peering.
Recovery	Peering will be re-established with the offending peer.

7 CALLTRACE

7.1 tmnxCallTraceLocSizeLimitReached

Table 131: tmnxCallTraceLocSizeLimitReached properties

Property name	Value
Application name	CALLTRACE
Event ID	2002
Event name	tmnxCallTraceLocSizeLimitReached
SNMP notification prefix and OID	TIMETRA-CALLTRACE-MIB.tmnxCallTraceNotifications.2
Default severity	minor
Message format string	Size limit (*$tmnxCallTraceLocationSizeLimit$* MB) of all call trace log files on 'cf *$tmnxCallTraceLocationCFlashId$*' has been reached
Cause	This notification is triggered when the cumulative size of all call trace log files on a given cflash card on the active CPM has reached the limit specified by the value of the object tmnxCallTraceLocationSizeLimit.
Effect	New call trace log file(s) cannot be created on the impacted cflash card.
Recovery	Operator may execute one of the following actions to restore the functionality: 1) Remove some call trace log files from the cflash card. 2) Increase the size limit (value of the object tmnxCallTraceLocation SizeLimit) for the given cflash card.

7.2 tmnxCallTraceMaxFilesNumReached

Table 132: tmnxCallTraceMaxFilesNumReached properties

Property name	Value
Application name	CALLTRACE
Event ID	2001
Event name	tmnxCallTraceMaxFilesNumReached
SNMP notification prefix and OID	TIMETRA-CALLTRACE-MIB.tmnxCallTraceNotifications.1

Property name	Value
Default severity	minor
Message format string	Cumulative limit of *$tmnxCallTraceMaxFilesNumber$* call trace log files on all cflash cards on the active CPM has been reached
Cause	This notification is triggered for the following reasons: 1) Cumulative number of call trace log files present on all cflash cards on the active CPM that are being used for their local storage has reached the limit defined by the value of the object tmnxCallTraceMaxFilesNumber. 2) The value of the object tmnxCallTraceMaxFilesNumber has been changed to a value that is lower than the current cumulative number of all call trace log files present on all cflash cards on the active CPM that are being used for their local storage. Details about cflash cards that are being used for the local storage of call trace log files can be found in tmnxCallTraceLocationTable.
Effect	New call trace log file(s) cannot be created on any cflash card.
Recovery	Operator may execute one of the following actions to restore the functionality: 1) Remove some call trace log files from (a) cflash card(s). 2) Increase the value of the object tmnxCallTraceMaxFiles Number.

8 CFLOWD

8.1 tmnxCflowdCreateFailure

Table 133: tmnxCflowdCreateFailure properties

Property name	Value
Application name	CFLOWD
Event ID	2002
Event name	tmnxCflowdCreateFailure
SNMP notification prefix and OID	TIMETRA-CFLOWD-MIB.tmnxCflowdNotifications.2
Default severity	minor
Message format string	Cflowd creation failed
Cause	The tmnxCflowdCreateFailure event is generated when Cflowd instance creation fails on the system.
Effect	cflowd is not running.
Recovery	Contact Nokia customer service.

8.2 tmnxCflowdFlowCreateFailure

Table 134: tmnxCflowdFlowCreateFailure properties

Property name	Value
Application name	CFLOWD
Event ID	2006
Event name	tmnxCflowdFlowCreateFailure
SNMP notification prefix and OID	TIMETRA-CFLOWD-MIB.tmnxCflowdNotifications.6
Default severity	minor
Message format string	Cflowd flow creation failed - *$tmnxCflowdFlowFailureReasonCode$*

Property name	Value
Cause	The tmnxCflowdFlowCreateFailure event is generated when the creation of a Cflowd flow fails.
Effect	Flow data may be lost.
Recovery	N/A

8.3 tmnxCflowdPacketTxFailure

Table 135: tmnxCflowdPacketTxFailure properties

Property name	Value
Application name	CFLOWD
Event ID	2009
Event name	tmnxCflowdPacketTxFailure
SNMP notification prefix and OID	TIMETRA-CFLOWD-MIB.tmnxCflowdNotifications.9
Default severity	minor
Message format string	Cflowd failed to send packet to collector *$tmnxCFHostCollAddress $*:*$tmnxCFHostCollUdpPort$* Version *$tmnxCFHostCollVersion$* - Reason: *$tmnxCflowdFlowFailureReasonCode$*
Cause	The tmnxCflowdPacketTxFailure event is generated when a cflowd packet fails to transmit from an active collector host.
Effect	Flow data may be lost.
Recovery	N/A

8.4 tmnxCflowdStateChange

Table 136: tmnxCflowdStateChange properties

Property name	Value
Application name	CFLOWD
Event ID	2004
Event name	tmnxCflowdStateChange
SNMP notification prefix and OID	TIMETRA-CFLOWD-MIB.tmnxCflowdNotifications.4

Property name	Value
Default severity	minor
Message format string	Status of cflowd changes to administrative state: *$tmnxCflowdAdmin Status$*, operational state: *$tmnxCflowdOperStatus$*
Cause	The tmnxCflowdStateChange event is triggered when tmnxCflowd AdminStatus or tmnxCflowdOperStatus reports a change.
Effect	N/A
Recovery	N/A

9 CHASSIS

9.1 CpmIcPortSFFStatusDDMCorrupt

Table 137: CpmIcPortSFFStatusDDMCorrupt properties

Property name	Value
Application name	CHASSIS
Event ID	4012
Event name	CpmIcPortSFFStatusDDMCorrupt
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.7
Default severity	minor
Message format string	CPM interconnect port SFF DDM checksums do not match
Cause	The tmnxCpmIcPortSFFStatusFailure notification is generated when the value of tmnxCpmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated CPM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.2 CpmIcPortSFFStatusFailure

Table 138: CpmIcPortSFFStatusFailure properties

Property name	Value
Application name	CHASSIS
Event ID	4011
Event name	CpmIcPortSFFStatusFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.7

Property name	Value
Default severity	minor
Message format string	CPM interconnect port SFF checksums do not match
Cause	The tmnxCpmIcPortSFFStatusFailure notification is generated when the value of tmnxCpmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated CPM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.3 CpmIcPortSFFStatusReadError

Table 139: CpmIcPortSFFStatusReadError properties

Property name	Value
Application name	CHASSIS
Event ID	4013
Event name	CpmIcPortSFFStatusReadError
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.7
Default severity	minor
Message format string	CPM interconnect port SFF read failure
Cause	The tmnxCpmIcPortSFFStatusFailure notification is generated when the value of tmnxCpmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated CPM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.4 CpmIcPortSFFStatusUnsupported

Table 140: CpmIcPortSFFStatusUnsupported properties

Property name	Value
Application name	CHASSIS
Event ID	4014
Event name	CpmIcPortSFFStatusUnsupported
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.7
Default severity	minor
Message format string	CPM interconnect port SFF unsupported type
Cause	The tmnxCpmIcPortSFFStatusFailure notification is generated when the value of tmnxCpmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated CPM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.5 SfmIcPortSFFStatusDDMCorrupt

Table 141: SfmIcPortSFFStatusDDMCorrupt properties

Property name	Value
Application name	CHASSIS
Event ID	4022
Event name	SfmIcPortSFFStatusDDMCorrupt
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.5
Default severity	minor
Message format string	SFM interconnect port SFF DDM checksums do not match

Property name	Value
Cause	The tmnxSfmIcPortSFFStatusFailure notification is generated when the value of tmnxSfmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated SFM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.6 SfmIcPortSFFStatusFailure

Table 142: SfmIcPortSFFStatusFailure properties

Property name	Value
Application name	CHASSIS
Event ID	4021
Event name	SfmIcPortSFFStatusFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.5
Default severity	minor
Message format string	SFM interconnect port SFF checksums do not match
Cause	The tmnxSfmIcPortSFFStatusFailure notification is generated when the value of tmnxSfmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated SFM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.7 SfmIcPortSFFStatusReadError

Table 143: SfmIcPortSFFStatusReadError properties

Property name	Value
Application name	CHASSIS
Event ID	4023
Event name	SfmIcPortSFFStatusReadError
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.5
Default severity	minor
Message format string	SFM interconnect port SFF read failure
Cause	The tmnxSfmIcPortSFFStatusFailure notification is generated when the value of tmnxSfmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated SFM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.8 SfmIcPortSFFStatusUnsupported

Table 144: SfmIcPortSFFStatusUnsupported properties

Property name	Value
Application name	CHASSIS
Event ID	4024
Event name	SfmIcPortSFFStatusUnsupported
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.5
Default severity	minor
Message format string	SFM interconnect port SFF unsupported type

Property name	Value
Cause	The tmnxSfmIcPortSFFStatusFailure notification is generated when the value of tmnxSfmIcPortSFFStatus results in a value other than 'not-equipped (0)', or 'operational (1)'.
Effect	The SFF device is not operational and the associated SFM interconnect port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

9.9 tIPsecIsaMemHighWatermark

Table 145: tIPsecIsaMemHighWatermark properties

Property name	Value
Application name	CHASSIS
Event ID	2151
Event name	tIPsecIsaMemHighWatermark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.138
Default severity	minor
Message format string	The memory usage ratio for ISA *$tmnxCardSlotNum$*/*$tmnxMDASlot Num$* has almost reached the maximum value.
Cause	A tIPsecIsaMemHighWatermark notification is generated when the ISA card memory usage ratio has almost reached the maximum value.
Effect	The system may stop accepting new IKE states shortly.
Recovery	Use fewer SAs for each IKE tunnel.

9.10 tIPsecIsaMemLowWatermark

Table 146: tIPsecIsaMemLowWatermark properties

Property name	Value
Application name	CHASSIS
Event ID	2150

Property name	Value
Event name	tIPsecIsaMemLowWatermark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.137
Default severity	minor
Message format string	The memory usage ratio for ISA *$tmnxCardSlotNum$*/*$tmnxMDASlot Num$* has dropped back to the normal level.
Cause	A tIPsecIsaMemLowWatermark notification is generated when the ISA card memory usage ratio has dropped back to the normal level.
Effect	The system accepts new IKE states.
Recovery	There is no recovery required for this notification.

9.11 tIPsecIsaMemMax

Table 147: tIPsecIsaMemMax properties

Property name	Value
Application name	CHASSIS
Event ID	2152
Event name	tIPsecIsaMemMax
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.139
Default severity	minor
Message format string	The memory usage for ISA *$tmnxCardSlotNum$*/*$tmnxMDASlotNum$* has reached the maximum value.
Cause	A tIPsecIsaMemMax notification is generated when the ISA card memory usage ratio has reached the maximum value.
Effect	The system stops accepting new IKE states.
Recovery	Use fewer SAs for each IKE tunnel.

9.12 tmnxAlarmInputVoltageFailure

Table 148: tmnxAlarmInputVoltageFailure properties

Property name	Value
Application name	CHASSIS
Event ID	3014
Event name	tmnxAlarmInputVoltageFailure
SNMP notification prefix and OID	TIMETRA-SAS-ALARM-INPUT-MIB.tmnxSASChassisNotification.10
Default severity	major
Message format string	Class *$tmnxHwClass$* : alarm input voltage failure
Cause	A tmnxAlarmInputVoltageFailure notification is sent when the internal power supply for alarm inputs fails. The value of tmnxSasAlarmInput PowerStatus indicates whether the power to external alarm inputs is on or off.
Effect	If the alarm inputs use the internal power supply, then a failure in the power supply will cause state change event alarms to not be raised.
Recovery	Check the internal power source for alarm inputs and rectify the problem.

9.13 tmnxChassisHiBwMcastAlarm

Table 149: tmnxChassisHiBwMcastAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2052
Event name	tmnxChassisHiBwMcastAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.43
Default severity	minor
Message format string	Class *$tmnxHwClass$* : Plane shared by multiple multicast high bandwidth taps
Cause	The tmnxChassisHiBwMcastAlarm notification is generated when a plane is shared by more than one high bandwidth multicast tap.
Effect	N/A

Property name	Value
Recovery	N/A

9.14 tmnxChassisNotificationClear

Table 150: tmnxChassisNotificationClear properties

Property name	Value
Application name	CHASSIS
Event ID	2016
Event name	tmnxChassisNotificationClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.25
Default severity	major
Message format string	Clear *$tmnxHwClass$ $tmnxHwIndex$ $tmnxChassisNotifyOID$*
Cause	A trap indicating the clear of a chassis notification identified by tmnx ChassisNotifyOID.
Effect	N/A
Recovery	N/A

9.15 tmnxChassisUpgradeComplete

Table 151: tmnxChassisUpgradeComplete properties

Property name	Value
Application name	CHASSIS
Event ID	2034
Event name	tmnxChassisUpgradeComplete
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.42
Default severity	major
Message format string	Class *$tmnxHwClass$* : software upgrade complete
Cause	The tmnxChassisUpgradeComplete notification is generated to indicate that all the IOMs are running matching software versions in reference

Property name	Value
	to the active CPM software version changed as part of the upgrade process.
Effect	N/A
Recovery	N/A

9.16 tmnxChassisUpgradeInProgress

Table 152: tmnxChassisUpgradeInProgress properties

Property name	Value
Application name	CHASSIS
Event ID	2033
Event name	tmnxChassisUpgradeInProgress
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.41
Default severity	major
Message format string	Class *$tmnxHwClass$* : software upgrade in progress
Cause	The tmnxChassisUpgradeInProgress notification is generated only after a CPM switchover occurs and the new active CPM is running new software, while the IOMs are still running old software. This is the start of the upgrade process. The tmnxChassisUpgradeInProgress notification will continue to be generated every 30 minutes while at least one IOM is still running older software.
Effect	N/A
Recovery	N/A

9.17 tmnxCpmALocalIcPortAvail

Table 153: tmnxCpmALocalIcPortAvail properties

Property name	Value
Application name	CHASSIS
Event ID	4009
Event name	tmnxCpmALocalIcPortAvail

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.6
Default severity	major
Message format string	CPM *$tmnxChassisNotifyCpmCardSlotNum$* can reach the chassis using its local CPM interconnect ports
Cause	The tmnxCpmLocalIcPortAvail notification is generated when the CPM re-establishes communication with the other chassis using its local CPM interconnect ports.
Effect	A new control communications path is now available between the CPM and the other chassis.
Recovery	N/A

9.18 tmnxCpmANoLocalIcPort

Table 154: tmnxCpmANoLocalIcPort properties

Property name	Value
Application name	CHASSIS
Event ID	4007
Event name	tmnxCpmANoLocalIcPort
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.5
Default severity	major
Message format string	CPM *$tmnxChassisNotifyCpmCardSlotNum$* can not reach the chassis using its local CPM interconnect ports
Cause	The tmnxCpmNoLocalIcPort alarm is generated when the CPM cannot reach the other chassis using its local CPM interconnect ports.
Effect	Another control communications path may still be available between the CPM and the other chassis via the mate CPM in the same chassis. If that alternative path is not available then complete disruption of control communications to the other chassis will occur and the tmnx InterChassisCommsDown alarm is raised. A tmnxCpmNoLocalIcPort alarm on the active CPM indicates that a further failure of the local CPM interconnect ports on the standby CPM will cause complete disruption of control communications to the other chassis and the tmnx InterChassisCommsDown alarm is raised. A tmnxCpmNoLocalIcPort

Property name	Value
	alarm on the standby CPM indicates that a CPM switchover may cause temporary disruption of control communications to the other chassis while the rebooting CPM comes back into service.
Recovery	Ensure that all CPM interconnect ports in the system are properly cabled together with working cables.

9.19 tmnxCpmBLocalIcPortAvail

Table 155: tmnxCpmBLocalIcPortAvail properties

Property name	Value
Application name	CHASSIS
Event ID	4010
Event name	tmnxCpmBLocalIcPortAvail
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.6
Default severity	major
Message format string	CPM *$tmnxChassisNotifyCpmCardSlotNum$* can reach the chassis using its local CPM interconnect ports
Cause	The tmnxCpmLocalIcPortAvail notification is generated when the CPM re-establishes communication with the other chassis using its local CPM interconnect ports.
Effect	A new control communications path is now available between the CPM and the other chassis.
Recovery	N/A

9.20 tmnxCpmBNoLocalIcPort

Table 156: tmnxCpmBNoLocalIcPort properties

Property name	Value
Application name	CHASSIS
Event ID	4008
Event name	tmnxCpmBNoLocalIcPort

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.5
Default severity	major
Message format string	CPM *$tmnxChassisNotifyCpmCardSlotNum$* can not reach the chassis using its local CPM interconnect ports
Cause	The tmnxCpmNoLocalIcPort alarm is generated when the CPM cannot reach the other chassis using its local CPM interconnect ports.
Effect	Another control communications path may still be available between the CPM and the other chassis via the mate CPM in the same chassis. If that alternative path is not available then complete disruption of control communications to the other chassis will occur and the tmnx InterChassisCommsDown alarm is raised. A tmnxCpmNoLocalIcPort alarm on the active CPM indicates that a further failure of the local CPM interconnect ports on the standby CPM will cause complete disruption of control communications to the other chassis and the tmnx InterChassisCommsDown alarm is raised. A tmnxCpmNoLocalIcPort alarm on the standby CPM indicates that a CPM switchover may cause temporary disruption of control communications to the other chassis while the rebooting CPM comes back into service.
Recovery	Ensure that all CPM interconnect ports in the system are properly cabled together with working cables.

9.21 tmnxCpmCardSyncFileNotPresent

Table 157: tmnxCpmCardSyncFileNotPresent properties

Property name	Value
Application name	CHASSIS
Event ID	2057
Event name	tmnxCpmCardSyncFileNotPresent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.45
Default severity	minor
Message format string	Class *$tmnxHwClass$* : Optional file *$tmnxChassisNotifyCardSyncFile $* is not present during sync operation
Cause	The tmnxCpmCardSyncFileNotPresent notification is generated when the redundancy file synchronization failed to locate an optional file.

Property name	Value
Effect	N/A
Recovery	N/A

9.22 tmnxCpmIcPortDDMClear

Table 158: tmnxCpmIcPortDDMClear properties

Property name	Value
Application name	CHASSIS
Event ID	4016
Event name	tmnxCpmIcPortDDMClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.9
Default severity	minor
Message format string	CPM interconnect port SFF DDM *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailedObject$*) cleared
Cause	The tmnxCpmIcPortDDMFailure notification is generated when an SFF in a CPM interconnect port that supports Digital Diagnostic Monitoring (DDM) clears a failed state.
Effect	N/A
Recovery	N/A

9.23 tmnxCpmIcPortDDMFailure

Table 159: tmnxCpmIcPortDDMFailure properties

Property name	Value
Application name	CHASSIS
Event ID	4015
Event name	tmnxCpmIcPortDDMFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.8

Property name	Value
Default severity	minor
Message format string	CPM interconnect port SFF DDM *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailedObject$*) raised
Cause	The tmnxCpmIcPortDDMFailure notification is generated when an SFF in a CPM interconnect port that supports Digital Diagnostic Monitoring (DDM) enters a failed state.
Effect	N/A
Recovery	N/A

9.24 tmnxCpmIcPortDown

Table 160: tmnxCpmIcPortDown properties

Property name	Value
Application name	CHASSIS
Event ID	4003
Event name	tmnxCpmIcPortDown
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.1
Default severity	minor
Message format string	CPM interconnect port is not operational. Error code = *$tmnxCpmIcPort OperState$*
Cause	The tmnxCpmIcPortDown alarm is generated when the CPM interconnect port is not operational. The reason may be a cable connected incorrectly, a disconnected cable, a faulty cable, or a misbehaving CPM interconnect port or card.
Effect	At least one of the control plane paths used for inter-chassis CPM communication is not operational. Other paths may be available.
Recovery	A manual verification and testing of each CPM interconnect port is required to ensure fully functional operation. Physical replacement of cabling may be required.

9.25 tmnxCpmIcPortSFFInserted

Table 161: tmnxCpmIcPortSFFInserted properties

Property name	Value
Application name	CHASSIS
Event ID	4005
Event name	tmnxCpmIcPortSFFInserted
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.3
Default severity	minor
Message format string	CPM interconnect port SFF inserted
Cause	The tmnxCpmIcPortSFFInserted notification is generated when the small form factor (SFF) pluggable optical module (eg. QSFP) is inserted into a CPM interconnect port.
Effect	This event is for notification only.
Recovery	N/A

9.26 tmnxCpmIcPortSFFRemoved

Table 162: tmnxCpmIcPortSFFRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	4006
Event name	tmnxCpmIcPortSFFRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.4
Default severity	minor
Message format string	CPM interconnect port SFF removed
Cause	The tmnxCpmIcPortSFFRemoved notification is generated when the SFF (eg. QSFP) is removed from the CPM interconnect port. Removing an SFF causes both this trap, and also a tmnxCpmIcPortDown event.

Property name	Value
Effect	Removing the SFF will cause the CPM interconnect port to go down. This port will no longer be able to be used as part of the control plane between chassis but other paths may be available.
Recovery	Insert a working SFF into the port.

9.27 tmnxCpmIcPortUp

Table 163: tmnxCpmIcPortUp properties

Property name	Value
Application name	CHASSIS
Event ID	4004
Event name	tmnxCpmIcPortUp
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.2
Default severity	minor
Message format string	CPM interconnect port is operational
Cause	The tmnxCpmIcPortUp notification is generated when the CPM interconnect port is operational again.
Effect	A control plane communication path between CPM cards in the different chassis have been established.
Recovery	N/A

9.28 tmnxCpmMemSizeMismatch

Table 164: tmnxCpmMemSizeMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2153
Event name	tmnxCpmMemSizeMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.140

Property name	Value
Default severity	major
Message format string	The standby CPM *$tmnxChassisNotifyCpmCardSlotNum$* has a different memory size than the active *$tmnxChassisNotifyHwIndex$*
Cause	A tmnxCpmMemSizeMismatch notification is generated when the RAM memory size of the standby CPM (i.e., tmnxChassisNotifyCpmCard SlotNum) is different than the active CPM (i.e., tmnxChassisNotify HwIndex).
Effect	There is an increased risk of the memory overflow on the standby CPM during the CPM switchover.
Recovery	Use CPMs with the same memory size.

9.29 tmnxCpmMemSizeMismatchClear

Table 165: tmnxCpmMemSizeMismatchClear properties

Property name	Value
Application name	CHASSIS
Event ID	2154
Event name	tmnxCpmMemSizeMismatchClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.141
Default severity	cleared
Message format string	The standby CPM *$tmnxChassisNotifyCpmCardSlotNum$* has the same memory size as the active *$tmnxChassisNotifyHwIndex$*
Cause	A tmnxCpmMemSizeMismatchClear notification is generated when the RAM memory sizes of the standby (i.e., tmnxChassisNotifyCpmCard SlotNum) and active (i.e., tmnxChassisNotifyHwIndex) CPMs become matched.
Effect	The tmnxCpmMemSizeMismatch notification is cleared.
Recovery	There is no recovery required for this notification.

9.30 tmnxDcpCardFpEventOvrflw

Table 166: tmnxDcpCardFpEventOvrflw properties

Property name	Value
Application name	CHASSIS
Event ID	2084
Event name	tmnxDcpCardFpEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.72
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpCardFpEventOvrflw notification is generated when a flood of distibuted CPU FP protection events occur on a particular card and some of the events are lost due to event throttling mechanism.
Effect	Some FP notifications configured on the card may not be received.
Recovery	Notifications will resume once the event throttling ends.

9.31 tmnxDcpCardFpEventOvrflwClr

Table 167: tmnxDcpCardFpEventOvrflwClr properties

Property name	Value
Application name	CHASSIS
Event ID	2089
Event name	tmnxDcpCardFpEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.77
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpCardFpEventOvrflwClr notification is generated when the event throttling has ended for distibuted CPU protection FP events on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

9.32 tmnxDcpCardSapEventOvrflw

Table 168: tmnxDcpCardSapEventOvrflw properties

Property name	Value
Application name	CHASSIS
Event ID	2085
Event name	tmnxDcpCardSapEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.73
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpCardSapEventOvrflw notification is generated when a flood of distibuted CPU protection SAP events occur on a particular card and some of the events are lost due to event throttling mechanism.
Effect	Some SAP notifications configured on the card may not be received.
Recovery	Notifications will resume once the event throttling ends.

9.33 tmnxDcpCardSapEventOvrflwClr

Table 169: tmnxDcpCardSapEventOvrflwClr properties

Property name	Value
Application name	CHASSIS
Event ID	2090
Event name	tmnxDcpCardSapEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.78
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpCardSapEventOvrflwClr notification is generated when the event throttling has ended for distibuted CPU protection SAP events on a particular card.
Effect	Notifications are received again since the event throttling has ended.

Property name	Value
Recovery	There is no recovery for this notification.

9.34 tmnxDcpCardVrtrIfEventOvrflw

Table 170: tmnxDcpCardVrtrIfEventOvrflw properties

Property name	Value
Application name	CHASSIS
Event ID	2086
Event name	tmnxDcpCardVrtrIfEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.74
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpCardVrtrIfEventOvrflw notification is generated when a flood of distibuted CPU protection network-interface events occur on a particular card and some of the events are lost due to event throttling mechanism.
Effect	Some network-interface notifications configured on the card may not be received.
Recovery	Notifications will resume once the event throttling ends.

9.35 tmnxDcpCardVrtrIfEventOvrflwClr

Table 171: tmnxDcpCardVrtrIfEventOvrflwClr properties

Property name	Value
Application name	CHASSIS
Event ID	2091
Event name	tmnxDcpCardVrtrIfEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.79
Default severity	minor
Message format string	TODO

Property name	Value
Cause	The tmnxDcpCardVrtrIfEventOvrflwClr notification is generated when the event throttling has ended for distibuted CPU protection networrk-interface events on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

9.36 tmnxDcpFpDynPoolUsageHiAlmClear

Table 172: tmnxDcpFpDynPoolUsageHiAlmClear properties

Property name	Value
Application name	CHASSIS
Event ID	2088
Event name	tmnxDcpFpDynPoolUsageHiAlmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.76
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpFpDynPoolUsageHiAlmClear notification is generated when the dynamic enforcement policer pool usage on the forwarding plane is no longer exhausted.
Effect	Dynamic enforcement policers are available in the free pool to be allocated when needed.
Recovery	There is no recovery required for this notification.

9.37 tmnxDcpFpDynPoolUsageHiAlmRaise

Table 173: tmnxDcpFpDynPoolUsageHiAlmRaise properties

Property name	Value
Application name	CHASSIS
Event ID	2087
Event name	tmnxDcpFpDynPoolUsageHiAlmRaise

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.75
Default severity	minor
Message format string	TODO
Cause	The tmnxDcpFpDynPoolUsageHiAlmRaise notification is generated when the dynamic enforcement policer pool usage on the forwarding plane is nearly exhausted.
Effect	Dynamic enforcement policers may not get allocated on the forwarding plane.
Recovery	This notification will be cleared when either the dynamic enforcement policer pool is increased or the usage drops.

9.38 tmnxEnvTempTooHigh

Table 174: tmnxEnvTempTooHigh properties

Property name	Value
Application name	CHASSIS
Event ID	2005
Event name	tmnxEnvTempTooHigh
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.2
Default severity	major
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: temperature too high
Cause	N/A
Effect	N/A
Recovery	N/A

9.39 tmnxEqCardChipIfCellEvent

Table 175: tmnxEqCardChipIfCellEvent properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2103
Event name	tmnxEqCardChipIfCellEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.90
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* experienced internal datapath cell errors • Slot *$tmnxHwIndex$* experienced internal datapath cell errors on complex *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardChipIfCellEvent notification is generated when an inter-chip interface (XPL2 bundle) experiences internal datapath cell errors.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

9.40 tmnxEqCardChipIfDownEvent

Table 176: tmnxEqCardChipIfDownEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2102
Event name	tmnxEqCardChipIfDownEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.89
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* experienced an internal datapath problem • Slot *$tmnxHwIndex$* experienced an internal datapath problem on complex *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardChipIfDownEvent notification is generated when an inter-chip interface (XPL2 bundle) experiences an internal datapath problem.
Effect	Contact Nokia customer support.

Property name	Value
Recovery	Contact Nokia customer support.

9.41 tmnxEqCardFailure

Table 177: tmnxEqCardFailure properties

Property name	Value
Application name	CHASSIS
Event ID	2001
Event name	tmnxEqCardFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.7
Default severity	major
Message format string	Class *$tmnxHwClass$* : failed, reason: *$tmnxChassisNotifyCardFailureReason$*
Cause	Generated when one of the cards in a chassis has failed. The card type may be IOM, Fabric, MDA, MCM, CCM, CPM module, compact flash module, etc. tmnxChassisNotifyCardFailureReason contains the reason for card failure.
Effect	N/A
Recovery	N/A

9.42 tmnxEqCardFirmwareUpgraded

Table 178: tmnxEqCardFirmwareUpgraded properties

Property name	Value
Application name	CHASSIS
Event ID	2032
Event name	tmnxEqCardFirmwareUpgraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.40
Default severity	major
Message format string	Class *$tmnxHwClass$* : firmware upgraded

Property name	Value
Cause	Generated when a card is hot-inserted into the chassis and its firmware is automatically upgraded. The card type may be IOM or CPM module.
Effect	N/A
Recovery	N/A

9.43 tmnxEqCardInserted

Table 179: tmnxEqCardInserted properties

Property name	Value
Application name	CHASSIS
Event ID	2002
Event name	tmnxEqCardInserted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.8
Default severity	minor
Message format string	Class *$tmnxHwClass$* : inserted
Cause	Generated when a card is inserted into the chassis. The card type may be IOM, Fabric, MDA, MCM, CCM CPM module, compact flash module, etc.
Effect	N/A
Recovery	N/A

9.44 tmnxEqCardPChipCamEvent

Table 180: tmnxEqCardPChipCamEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2076
Event name	tmnxEqCardPChipCamEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.64

Property name	Value
Default severity	critical
Message format string	A fault has been detected in the hardware on IOM *$tmnxSlotNum$*-forwarding engine *$tmnxCardComplexNumber$*: Please contact Nokia support
Cause	The tmnxEqCardPChipCamEvent notification is generated when either an IOM or a CPM experiences a persistent occurrence of a PChip CAM error. On a CPM card, the tmnxCardComplexNumber will be fixed to the value zero (0).
Effect	N/A
Recovery	N/A

9.45 tmnxEqCardPChipError

Table 181: tmnxEqCardPChipError properties

Property name	Value
Application name	CHASSIS
Event ID	2059
Event name	tmnxEqCardPChipError
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.47
Default severity	minor
Message format string	Slot *$tmnxCardSlotNum$* detected *$tmnxCardFwdDirection$* FCS errors on complex *$tmnxCardComplexNumber$*. Source card(s) of detected errors: *$tmnxCardSrcSlotBitmap$*
Cause	The tmnxEqCardPChipError notification is generated when persistent FCS errors are detected by the P chip in either the ingress or egress datapath/complex. The value tmnxCardSrcSlotBitmap is only used for the egress datapath/complex direction.
Effect	N/A
Recovery	N/A

9.46 tmnxEqCardPChipMemoryEvent

Table 182: tmnxEqCardPChipMemoryEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2063
Event name	tmnxEqCardPChipMemoryEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.51
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* experienced a pchip memory error occurrence • Slot *$tmnxHwIndex$* experienced a pchip parity error occurrence on complex *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardPChipMemoryEvent notification is generated when a P-chip experiences an occurrence of a memory error.
Effect	N/A
Recovery	N/A

9.47 tmnxEqCardQChipBufMemoryEvent

Table 183: tmnxEqCardQChipBufMemoryEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2098
Event name	tmnxEqCardQChipBufMemoryEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.86
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* experienced a Q-chip buffer memory error occurrence • Slot *$tmnxHwIndex$* experienced a Q-chip buffer memory error occurrence on complex *$tmnxCardComplexNumber$*

Property name	Value
Cause	The tmnxEqCardQChipBufMemoryEvent notification is generated when a Q-chip experiences an occurrence of a buffer memory error.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

9.48 tmnxEqCardQChipIntMemoryEvent

Table 184: tmnxEqCardQChipIntMemoryEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2101
Event name	tmnxEqCardQChipIntMemoryEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.88
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* experienced a qchip internal memory error occurrence • Slot *$tmnxHwIndex$* experienced a qchip internal memory error occurrence on complex *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardQChipIntMemoryEvent notification is generated when a Q-chip experiences an occurrence of an internal memory error.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

9.49 tmnxEqCardQChipStatsMemoryEvent

Table 185: tmnxEqCardQChipStatsMemoryEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2099

Property name	Value
Event name	tmnxEqCardQChipStatsMemoryEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.87
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* experienced a Q-chip statistics memory error occurrence • Slot *$tmnxHwIndex$* experienced a Q-chip statistics memory error occurrence on complex *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardQChipStatsMemoryEvent notification is generated when a Q-chip experiences an occurrence of a statistics memory error.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

9.50 tmnxEqCardRemoved

Table 186: tmnxEqCardRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	2003
Event name	tmnxEqCardRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.9
Default severity	major
Message format string	Class *$tmnxHwClass$* : removed
Cause	Generated when a card is removed from the chassis. The card type may be IOM, Fabric, MDA, MCM, CCM, CPM module, compact flash module, etc.
Effect	N/A
Recovery	N/A

9.51 tmnxEqCardSoftResetAlarm

Table 187: tmnxEqCardSoftResetAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2060
Event name	tmnxEqCardSoftResetAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.48
Default severity	minor
Message format string	Slot *$tmnxHwIndex$* entered soft-reset state *$tmnxCardSoftResetState$*
Cause	The tmnxEqCardSoftResetAlarm notification is generated when an IOM card enters and exits the 'soft-reset' state.
Effect	N/A
Recovery	N/A

9.52 tmnxEqCardTChipParityEvent

Table 188: tmnxEqCardTChipParityEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2110
Event name	tmnxEqCardTChipParityEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.97
Default severity	minor
Message format string	Slot *$tmnxHwIndex$* experienced a T-chip memory error occurrence on complex *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardTChipParityEvent notification is generated when a T-chip experiences an occurrence of an internal memory error.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

9.53 tmnxEqDataPathFailureProtImpact

Table 189: tmnxEqDataPathFailureProtImpact properties

Property name	Value
Application name	CHASSIS
Event ID	2126
Event name	tmnxEqDataPathFailureProtImpact
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.113
Default severity	minor
Message format string	*$tmnxHwClass$ $tmnxHwIndex$* experienced a datapath failure which impacted a protocol.
Cause	The tmnxEqDataPathFailureProtImpact notification is generated when a slot experienced a data path failure which impacted a protocol.
Effect	Services-related data associated with the impacted protocol may be lost.
Recovery	N/A

9.54 tmnxEqFanFailure

Table 190: tmnxEqFanFailure properties

Property name	Value
Application name	CHASSIS
Event ID	2006
Event name	tmnxEqFanFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.6
Default severity	critical
Message format string	Fan *$tmnxChassisNotifyHwIndex$* failed
Cause	Generated when one of the fans in a fan tray has failed.
Effect	N/A
Recovery	N/A

9.55 tmnxEqFlashDataLoss

Table 191: tmnxEqFlashDataLoss properties

Property name	Value
Application name	CHASSIS
Event ID	2023
Event name	tmnxEqFlashDataLoss
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.32
Default severity	major
Message format string	Class *$tmnxHwClass$* : probable data loss
Cause	tmnxEqFlashDataLoss is generated when an error occurs while data was being written to the compact flash. This notification indicates a probable data loss.
Effect	N/A
Recovery	N/A

9.56 tmnxEqFlashDiskFull

Table 192: tmnxEqFlashDiskFull properties

Property name	Value
Application name	CHASSIS
Event ID	2024
Event name	tmnxEqFlashDiskFull
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.33
Default severity	major
Message format string	Class *$tmnxHwClass$* : disk full
Cause	tmnxEqFlashDiskFull is generated when there is no space left on the compact flash. No more data can be written to it.
Effect	N/A
Recovery	N/A

9.57 tmnxEqHwEnhancedCapability

Table 193: tmnxEqHwEnhancedCapability properties

Property name	Value
Application name	CHASSIS
Event ID	2078
Event name	tmnxEqHwEnhancedCapability
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.66
Default severity	major
Message format string	CPM Upgrade In Progress. Card in slot *$tmnxCardSlotNum$* has enhanced capabilities.
Cause	The tmnxEqHwEnhancedCapability notification is generated when the hardware, specified by the supplied objects, consists of enhanced capabilities as compared to the active hardware.
Effect	The system behaves normally under this situation, however, switching to the newer hardware will put the system in an incompatible state with the currently active hardware. That is, once this device takes activity, the lesser capable hardware will fail to communicate with it. In this mode, the system is deemed in a 'one-way upgrade' scenario.
Recovery	Two modes of recovery exist for this notification: 1) Remove the enhanced hardware, and supply a more compatible device (status quo) with the active hardware. 2) Switch to the enhanced device, and replace the older hardware with a similarly enhanced device (upgrade).

9.58 tmnxEqLowSwitchFabricCap

Table 194: tmnxEqLowSwitchFabricCap properties

Property name	Value
Application name	CHASSIS
Event ID	2104
Event name	tmnxEqLowSwitchFabricCap
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.91
Default severity	major

Property name	Value
Message format string	The switch fabric capacity is less than the forwarding capacity of *$tmnxHwClass$ $tmnxHwIndex$* due to errors in fabric links.
Cause	The tmnxEqLowSwitchFabricCap alarm is generated when the total switch fabric capacity becomes less than the IOM capacity due to link failures. At least one of the taps on the IOM is below 100% capacity.
Effect	There is diminished switch fabric capacity to forward service-impacting information.
Recovery	If the system does not self-recover, the IOM must be rebooted.

9.59 tmnxEqLowSwitchFabricCapClear

Table 195: tmnxEqLowSwitchFabricCapClear properties

Property name	Value
Application name	CHASSIS
Event ID	2105
Event name	tmnxEqLowSwitchFabricCapClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.92
Default severity	major
Message format string	The switch fabric capacity alarm for *$tmnxHwClass$ $tmnxHwIndex$* was cleared.
Cause	The tmnxEqLowSwitchFabricCapClear notification is generated when the link failures that resulted in the tmnxEqLowSwitchFabricCap alarm to be raised have been resolved.
Effect	There is sufficient switch fabric capacity to forward service-impacting information.
Recovery	N/A

9.60 tmnxEqMdaCfgNotCompatible

Table 196: tmnxEqMdaCfgNotCompatible properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2056
Event name	tmnxEqMdaCfgNotCompatible
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.44
Default severity	major
Message format string	Class *$tmnxHwClass$* : configuration not compatible with equipped MDA
Cause	Generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible with the currently provisioned MDA, but the current configuration on the MDA's ports is not compatible with the inserted MDA.
Effect	Though services can still be created, if the tmnxMdaNotifyType is the same as the tmnxMDAEquippedType then the MDA will fail to operate as configured and will be in a failed state.
Recovery	Change the configuration to reflect the capabilities of the MDA port, or switch out/re-provision the MDA for one that is compatible.

9.61 tmnxEqMdaIngrXplError

Table 197: tmnxEqMdaIngrXplError properties

Property name	Value
Application name	CHASSIS
Event ID	2129
Event name	tmnxEqMdaIngrXplError
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.116
Default severity	minor
Message format string	MDA *$tmnxCardSlotNum$*/ *$tmnxEqMdaSlotNum$* experienced an ingress XPL error occurrence.
Cause	The tmnxEqMdaIngrXplError notification is generated when an MDA exhibits persistent ingress XPL errors.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

9.62 tmnxEqMdaSyncENotCompatible

Table 198: tmnxEqMdaSyncENotCompatible properties

Property name	Value
Application name	CHASSIS
Event ID	2061
Event name	tmnxEqMdaSyncENotCompatible
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.49
Default severity	major
Message format string	Provisioned synchronous ethernet not compatible with equipped MDA
Cause	The tmnxEqMdaSyncENotCompatible notification is generated when an MDA card is inserted into a slot of an IOM. The MDA is compatible with the currently provisioned MDA, but the currently configured synchronous ethernet, tmnxMDASynchronousEthernet, is not compatible with the inserted MDA.
Effect	Though services can still be created, if the tmnxMdaNotifyType is the same as the tmnxMDAEquippedType then the MDA will fail to operate as configured and will be in a failed state.
Recovery	Change the configuration to reflect the capabilities of the MDA port, or switch out/re-provision the MDA for one that is compatible.

9.63 tmnxEqMdaXplError

Table 199: tmnxEqMdaXplError properties

Property name	Value
Application name	CHASSIS
Event ID	2058
Event name	tmnxEqMdaXplError
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.46
Default severity	minor
Message format string	MDA *$tmnxCardSlotNum$*/ *$tmnxMDASlotNum$* experienced an egress XPL error occurrence.

Property name	Value
Cause	The tmnxEqMdaXplError notification is generated when an MDA exhibits persistent egress XPL Errors.
Effect	N/A
Recovery	N/A

9.64 tmnxEqMgmtEthRedStandbyClear

Table 200: tmnxEqMgmtEthRedStandbyClear properties

Property name	Value
Application name	CHASSIS
Event ID	2137
Event name	tmnxEqMgmtEthRedStandbyClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.122
Default severity	minor
Message format string	The active CPM's management Ethernet port *$tmnxChassisNotifyMgmtEthRedPort$* is serving as the system's management Ethernet port.
Cause	The tmnxEqMgmtEthRedStandbyClear notification is generated when the active CPM's management Ethernet port goes operationally up and the management Ethernet port reverts from the standby CPM to the active CPM.
Effect	The management of the node is operating from the active CPM's management Ethernet port and is redundant.
Recovery	No recovery required.

9.65 tmnxEqMgmtEthRedStandbyRaise

Table 201: tmnxEqMgmtEthRedStandbyRaise properties

Property name	Value
Application name	CHASSIS
Event ID	2136
Event name	tmnxEqMgmtEthRedStandbyRaise

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.121
Default severity	minor
Message format string	The standby CPM's management Ethernet port *$tmnxChassisNotifyMgmtEthRedPort$* is serving as the system's management Ethernet port.
Cause	The tmnxEqMgmtEthRedStandbyRaise notification is generated when the active CPM's management Ethernet port goes operationally down and the standby CPM's management Ethernet port is operationally up and now serving as the system's management Ethernet port.
Effect	The management Ethernet port is no longer redundant. The node can be managed via the standby CPM's management Ethernet port only.
Recovery	Bring the active CPM's management Ethernet port operationally up.

9.66 tmnxEqPhysChassisFanFailure

Table 202: tmnxEqPhysChassisFanFailure properties

Property name	Value
Application name	CHASSIS
Event ID	2148
Event name	tmnxEqPhysChassisFanFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.135
Default severity	critical
Message format string	Chassis *$tmnxPhysChassisNum$* fan *$tmnxPhysChassisFanIndex$* failure
Cause	The tmnxEqPhysChassisFanFailure notification is generated when one of the fans in a fan tray fails on a particular physical chassis.
Effect	The fan is no longer operational.
Recovery	Insert a new fan.

9.67 tmnxEqPhysChassisFanFailureClear

Table 203: tmnxEqPhysChassisFanFailureClear properties

Property name	Value
Application name	CHASSIS
Event ID	2149
Event name	tmnxEqPhysChassisFanFailureClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.136
Default severity	cleared
Message format string	Chassis *$tmnxPhysChassisNum$* fan *$tmnxPhysChassisFanIndex$* failure cleared
Cause	The tmnxEqPhysChassisFanFailureClear notification is generated when the fan failure is cleared on the particular physical chassis.
Effect	The fan is operational again.
Recovery	There is no recovery for this notification.

9.68 tmnxEqPhysChassPowerSupAcFail

Table 204: tmnxEqPhysChassPowerSupAcFail properties

Property name	Value
Application name	CHASSIS
Event ID	2140
Event name	tmnxEqPhysChassPowerSupAcFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.127
Default severity	critical
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* AC failure
Cause	The tmnxEqPhysChassPowerSupAcFail notification is generated when an AC failure occurs on the power supply.
Effect	The power supply is no longer operational.
Recovery	Insert a new power supply.

9.69 tmnxEqPhysChassPowerSupAcFailClr

Table 205: tmnxEqPhysChassPowerSupAcFailClr properties

Property name	Value
Application name	CHASSIS
Event ID	2141
Event name	tmnxEqPhysChassPowerSupAcFailClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.128
Default severity	cleared
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* AC failure cleared
Cause	The tmnxEqPhysChassPowerSupAcFailClr notification is generated when the AC failure is cleared on the power supply.
Effect	The power supply is operational again.
Recovery	There is no recovery for this notification.

9.70 tmnxEqPhysChassPowerSupDcFail

Table 206: tmnxEqPhysChassPowerSupDcFail properties

Property name	Value
Application name	CHASSIS
Event ID	2142
Event name	tmnxEqPhysChassPowerSupDcFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.129
Default severity	critical
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* DC failure
Cause	The tmnxEqPhysChassPowerSupDcFail notification is generated when a DC failure occurs on the power supply.
Effect	The power supply is no longer operational.

Property name	Value
Recovery	Insert a new power supply.

9.71 tmnxEqPhysChassPowerSupDcFailClr

Table 207: tmnxEqPhysChassPowerSupDcFailClr properties

Property name	Value
Application name	CHASSIS
Event ID	2143
Event name	tmnxEqPhysChassPowerSupDcFailClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.130
Default severity	cleared
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* DC failure cleared
Cause	The tmnxEqPhysChassPowerSupDcFailClr notification is generated when the DC failure is cleared on the power supply.
Effect	The power supply is operational again.
Recovery	There is no recovery for this notification.

9.72 tmnxEqPhysChassPowerSupInFail

Table 208: tmnxEqPhysChassPowerSupInFail properties

Property name	Value
Application name	CHASSIS
Event ID	2144
Event name	tmnxEqPhysChassPowerSupInFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.131
Default severity	critical
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* input failure

Property name	Value
Cause	The tmnxEqPhysChassPowerSupInFail notification is generated when an input failure occurs on the power supply.
Effect	The power supply is no longer operational.
Recovery	Check input feed and/or insert a new power supply.

9.73 tmnxEqPhysChassPowerSupInFailClr

Table 209: tmnxEqPhysChassPowerSupInFailClr properties

Property name	Value
Application name	CHASSIS
Event ID	2145
Event name	tmnxEqPhysChassPowerSupInFailClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.132
Default severity	cleared
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* input failure cleared
Cause	The tmnxEqPhysChassPowerSupInFailClr notification is generated when the input failure is cleared on the power supply.
Effect	The power supply is operational again.
Recovery	There is no recovery for this notification.

9.74 tmnxEqPhysChassPowerSupOutFail

Table 210: tmnxEqPhysChassPowerSupOutFail properties

Property name	Value
Application name	CHASSIS
Event ID	2146
Event name	tmnxEqPhysChassPowerSupOutFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.133

Property name	Value
Default severity	critical
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* output failure
Cause	The tmnxEqPhysChassPowerSupOutFail notification is generated when an output failure occurs on the power supply.
Effect	The power supply is no longer operational.
Recovery	Insert a new power supply.

9.75 tmnxEqPhysChassPowerSupOutFailCl

Table 211: tmnxEqPhysChassPowerSupOutFailCl properties

Property name	Value
Application name	CHASSIS
Event ID	2147
Event name	tmnxEqPhysChassPowerSupOutFailCl
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.134
Default severity	cleared
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* output failure cleared
Cause	The tmnxEqPhysChassPowerSupOutFailCl notification is generated when an output failure is cleared on the power supply.
Effect	The power supply is operational again.
Recovery	There is no recovery for this notification.

9.76 tmnxEqPhysChassPowerSupOvrTmp

Table 212: tmnxEqPhysChassPowerSupOvrTmp properties

Property name	Value
Application name	CHASSIS
Event ID	2138

Property name	Value
Event name	tmnxEqPhysChassPowerSupOvrTmp
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.125
Default severity	critical
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* over temperature
Cause	The tmnxEqPhysChassPowerSupOvrTmp notification is generated when a power supply's temperature surpasses the threshold of the particular physical chassis.
Effect	The power supply is no longer operational.
Recovery	Check input feed and/or insert a new power supply.

9.77 tmnxEqPhysChassPowerSupOvrTmpClr

Table 213: tmnxEqPhysChassPowerSupOvrTmpClr properties

Property name	Value
Application name	CHASSIS
Event ID	2139
Event name	tmnxEqPhysChassPowerSupOvrTmpClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.126
Default severity	cleared
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* over temperature cleared
Cause	The tmnxEqPhysChassPowerSupOvrTmpClr notification is generated when a power supply's temperature is reduced below the threshold of the particular physical chassis.
Effect	The power supply is operational again.
Recovery	There is no recovery for this notification.

9.78 tmnxEqPowerCapacityExceeded

Table 214: tmnxEqPowerCapacityExceeded properties

Property name	Value
Application name	CHASSIS
Event ID	2092
Event name	tmnxEqPowerCapacityExceeded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.80
Default severity	minor
Message format string	The system has reached maximum power capacity *$tmnxChassisNotifyPowerCapacity$* watts
Cause	The tmnxEqPowerCapacityExceeded alarm is generated when a device needs power to boot, but there is not enough power capacity to support the device.
Effect	A non-powered device will not boot until the power capacity is increased to support the device.
Recovery	Add a new power supply to the system or change the faulty power supply for a working one.

9.79 tmnxEqPowerCapacityExceededClear

Table 215: tmnxEqPowerCapacityExceededClear properties

Property name	Value
Application name	CHASSIS
Event ID	2093
Event name	tmnxEqPowerCapacityExceededClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.81
Default severity	minor
Message format string	The system power capacity is sufficient to support installed devices
Cause	The tmnxEqPowerCapacityExceededClear notification is generated when the available power capacity exceeds the required power to boot all inserted devices.
Effect	Devices that failed to boot due to power constrains, power up.

Property name	Value
Recovery	N/A

9.80 tmnxEqPowerLostCapacity

Table 216: tmnxEqPowerLostCapacity properties

Property name	Value
Application name	CHASSIS
Event ID	2094
Event name	tmnxEqPowerLostCapacity
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.82
Default severity	major
Message format string	The system can no longer support configured devices. Power capacity dropped to *$tmnxChassisNotifyPowerCapacity$* watts
Cause	The tmnxEqPowerLostCapacity alarm is generated when a power supply fails or is removed which puts the system in an overloaded situation.
Effect	Devices are powered off in order of lowest power priority (tmnxMDAHw PowerPriority) until the available power capacity can support the powered devices.
Recovery	Add a new power supply to the system or change the faulty power supply for a working one.

9.81 tmnxEqPowerLostCapacityClear

Table 217: tmnxEqPowerLostCapacityClear properties

Property name	Value
Application name	CHASSIS
Event ID	2095
Event name	tmnxEqPowerLostCapacityClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.83
Default severity	major

Property name	Value
Message format string	The system has reached a sustainable power capacity.
Cause	The tmnxEqPowerLostCapacityClear notification is generated when the available power capacity exceeds the required power to boot all inserted devices.
Effect	Devices that powered off due to power constrains, power up.
Recovery	N/A

9.82 tmnxEqPowerOverloadState

Table 218: tmnxEqPowerOverloadState properties

Property name	Value
Application name	CHASSIS
Event ID	2096
Event name	tmnxEqPowerOverloadState
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.84
Default severity	critical
Message format string	The system has reached critical power capacity. Increase available power now.
Cause	The tmnxEqPowerOverloadState alarm is generated when the overloaded power capacity can not support the power requirements and there are no further devices that can be powered off.
Effect	The system runs a risk of experiencing brownouts while the available power capacity does not meet the required power consumption.
Recovery	Add power capacity or manually shut down devices until the power capacity meets the power needs.

9.83 tmnxEqPowerOverloadStateClear

Table 219: tmnxEqPowerOverloadStateClear properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2097
Event name	tmnxEqPowerOverloadStateClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.85
Default severity	critical
Message format string	The system has reached a sustainable power capacity for critical equipment.
Cause	The tmnxEqPowerOverloadStateClear notification is generated when the available power capacity meets or exceeds the power needs of the powered on devices.
Effect	N/A
Recovery	N/A

9.84 tmnxEqPowerSafetyAlertClear

Table 220: tmnxEqPowerSafetyAlertClear properties

Property name	Value
Application name	CHASSIS
Event ID	2107
Event name	tmnxEqPowerSafetyAlertClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.94
Default severity	minor
Message format string	Possible messages: • The system power capacity safety alert for zone *$tmnxChassisPwrMgmtZone$* has been disabled. • The system power capacity for zone *$tmnxChassisPwrMgmtZone$* meets or exceeds the configured safety alert threshold of *$tmnxChassisPwrMgmtSafetyAlert$* watts.
Cause	The tmnxEqPowerSafetyAlertClear notification is generated when the system power capacity raises above the configured safety alert threshold.
Effect	This event is for notification only.
Recovery	N/A

9.85 tmnxEqPowerSafetyAlertThreshold

Table 221: tmnxEqPowerSafetyAlertThreshold properties

Property name	Value
Application name	CHASSIS
Event ID	2106
Event name	tmnxEqPowerSafetyAlertThreshold
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.93
Default severity	minor
Message format string	The system power capacity for zone *$tmnxChassisPwrMgmtZone$* dropped below the configured safety alert threshold of *$tmnxChassis PwrMgmtSafetyAlert$* watts.
Cause	The tmnxEqPowerSafetyAlertThreshold notification is generated when the system power capacity drops below the configured safety alert threshold.
Effect	This event is for notification only.
Recovery	N/A

9.86 tmnxEqPowerSafetyLevelClear

Table 222: tmnxEqPowerSafetyLevelClear properties

Property name	Value
Application name	CHASSIS
Event ID	2109
Event name	tmnxEqPowerSafetyLevelClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.96
Default severity	minor
Message format string	The peak nodal power for zone *$tmnxChassisPwrMgmtZone$* consumption dropped below the configured safety level threshold of *$tmnxChassisPwrMgmtSafetyLevel$* percent

Property name	Value
Cause	The tmnxEqPowerSafetyLevelClear notification is generated when the peak nodal power consumption drops below the configured safety level threshold.
Effect	This event is for notification only.
Recovery	N/A

9.87 tmnxEqPowerSafetyLevelThreshold

Table 223: tmnxEqPowerSafetyLevelThreshold properties

Property name	Value
Application name	CHASSIS
Event ID	2108
Event name	tmnxEqPowerSafetyLevelThreshold
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.95
Default severity	minor
Message format string	The peak nodal power for zone *$tmnxChassisPwrMgmtZone$* consumption exceeded the configured safety level threshold of *$tmnx ChassisPwrMgmtSafetyLevel$* percent
Cause	The tmnxEqPowerSafetyLevelThreshold notification is generated when the peak nodal power consumption exceeds the configured safety level threshold.
Effect	This event is for notification only.
Recovery	N/A

9.88 tmnxEqPowerSupplyFailureAc

Table 224: tmnxEqPowerSupplyFailureAc properties

Property name	Value
Application name	CHASSIS
Event ID	2008
Event name	tmnxEqPowerSupplyFailureAc

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.3
Default severity	critical
Message format string	Power supply *$tmnxChassisNotifyHwIndex$* AC failure
Cause	Generated when the temperature sensor reading on an equipment object is greater than its configured threshold.
Effect	N/A
Recovery	N/A

9.89 tmnxEqPowerSupplyFailureDc

Table 225: tmnxEqPowerSupplyFailureDc properties

Property name	Value
Application name	CHASSIS
Event ID	2009
Event name	tmnxEqPowerSupplyFailureDc
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.3
Default severity	critical
Message format string	Power supply *$tmnxChassisNotifyHwIndex$* DC failure
Cause	Generated when one of the chassis's power supplies fails.
Effect	N/A
Recovery	N/A

9.90 tmnxEqPowerSupplyFailureInput

Table 226: tmnxEqPowerSupplyFailureInput properties

Property name	Value
Application name	CHASSIS
Event ID	2050

Property name	Value
Event name	tmnxEqPowerSupplyFailureInput
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.3
Default severity	critical
Message format string	Power supply *$tmnxChassisNotifyHwIndex$* input failure
Cause	Generated when one of the chassis's power supplies fails.
Effect	N/A
Recovery	N/A

9.91 tmnxEqPowerSupplyFailureOutput

Table 227: tmnxEqPowerSupplyFailureOutput properties

Property name	Value
Application name	CHASSIS
Event ID	2051
Event name	tmnxEqPowerSupplyFailureOutput
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.3
Default severity	critical
Message format string	Power supply *$tmnxChassisNotifyHwIndex$* output failure
Cause	Generated when one of the chassis's power supplies fails.
Effect	N/A
Recovery	N/A

9.92 tmnxEqPowerSupplyFailureOvt

Table 228: tmnxEqPowerSupplyFailureOvt properties

Property name	Value
Application name	CHASSIS
Event ID	2007

Property name	Value
Event name	tmnxEqPowerSupplyFailureOvt
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.3
Default severity	critical
Message format string	Power supply *$tmnxChassisNotifyHwIndex$* over temperature
Cause	N/A
Effect	N/A
Recovery	N/A

9.93 tmnxEqPowerSupplyInputFeedAlm

Table 229: tmnxEqPowerSupplyInputFeedAlm properties

Property name	Value
Application name	CHASSIS
Event ID	2113
Event name	tmnxEqPowerSupplyInputFeedAlm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.100
Default severity	minor
Message format string	Power supply *$tmnxHwIndex$ $tmnxChassisPowerSupplyInFeedDown $*not supplying power.
Cause	The tmnxEqPowerSupplyInputFeedAlm alarm is generated if any one of the input feeds for a given power supply is not supplying power.
Effect	There is an increased risk of system power brown-outs or black-outs.
Recovery	Restore all of the input feeds that are not supplying power.

9.94 tmnxEqPowerSupplyInputFeedAlmClr

Table 230: tmnxEqPowerSupplyInputFeedAlmClr properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2114
Event name	tmnxEqPowerSupplyInputFeedAlmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.101
Default severity	minor
Message format string	The input feeds for power supply *$tmnxHwIndex$* are supplying power.
Cause	The tmnxEqPowerSupplyInputFeedAlmClr notification is generated when the last of the missing input feeds has been brought back online.
Effect	All power supply input feeds are supplying power.
Recovery	N/A

9.95 tmnxEqPowerSupplyInserted

Table 231: tmnxEqPowerSupplyInserted properties

Property name	Value
Application name	CHASSIS
Event ID	2010
Event name	tmnxEqPowerSupplyInserted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.4
Default severity	major
Message format string	Power supply *$tmnxChassisNotifyHwIndex$* inserted
Cause	Generated when one of the chassis's power supplies is inserted.
Effect	N/A
Recovery	N/A

9.96 tmnxEqPowerSupplyPemACRectAlm

Table 232: tmnxEqPowerSupplyPemACRectAlm properties

Property name	Value
Application name	CHASSIS
Event ID	2111
Event name	tmnxEqPowerSupplyPemACRectAlm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.98
Default severity	minor
Message format string	Power supply *$tmnxHwIndex$ $tmnxChassisPowerSupplyPemACRect $*failed or missing.
Cause	The tmnxEqPowerSupplyPemACRectAlm alarm is generated if any one of the AC rectifiers for a given power supply is in a failed state or is missing.
Effect	There is an increased risk of the power supply failing, causing insufficient power to the system.
Recovery	Bring the AC rectifiers back online.

9.97 tmnxEqPowerSupplyPemACRectAlmClr

Table 233: tmnxEqPowerSupplyPemACRectAlmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2112
Event name	tmnxEqPowerSupplyPemACRectAlmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.99
Default severity	minor
Message format string	The power supply *$tmnxHwIndex$* AC rectifiers are fully operational.
Cause	The tmnxEqPowerSupplyPemACRectAlmClr notification is generated when the last of the failed or missing AC rectifiers has been brought back online.
Effect	The power supply AC rectifiers are fully operational.

Property name	Value
Recovery	N/A

9.98 tmnxEqPowerSupplyRemoved

Table 234: tmnxEqPowerSupplyRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	2011
Event name	tmnxEqPowerSupplyRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.5
Default severity	major
Message format string	Power supply *$tmnxChassisNotifyHwIndex$*, power lost
Cause	Generated when one of the chassis's power supplies is removed.
Effect	N/A
Recovery	N/A

9.99 tmnxEqProvPowerCapacityAlm

Table 235: tmnxEqProvPowerCapacityAlm properties

Property name	Value
Application name	CHASSIS
Event ID	2115
Event name	tmnxEqProvPowerCapacityAlm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.102
Default severity	minor
Message format string	The provisioned power capacity can no longer support configured devices.

Property name	Value
Cause	The tmnxEqProvPowerCapacityAlm notification is generated if a power zone's provisioned power capacity can no longer support configured devices.
Effect	There is an increased risk of device power outages that may be service affecting.
Recovery	Increase the provisioned power capacity.

9.100 tmnxEqProvPowerCapacityAlmClr

Table 236: tmnxEqProvPowerCapacityAlmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2116
Event name	tmnxEqProvPowerCapacityAlmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.103
Default severity	minor
Message format string	The provisioned power capacity now supports configured devices.
Cause	The tmnxEqProvPowerCapacityAlmClr notification is generated when the power zone's provisioned power capacity can support configured devices.
Effect	All configured devices in the power zone have enough provisioned power capacity.
Recovery	N/A

9.101 tmnxEqSyncIfTimingBITS2Alarm

Table 237: tmnxEqSyncIfTimingBITS2Alarm properties

Property name	Value
Application name	CHASSIS
Event ID	2073
Event name	tmnxEqSyncIfTimingBITS2Alarm

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.61
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on BITS 2 reference
Cause	Generated when an alarm condition on the BITS 2 timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.102 tmnxEqSyncIfTimingBITS2AlarmClr

Table 238: tmnxEqSyncIfTimingBITS2AlarmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2074
Event name	tmnxEqSyncIfTimingBITS2AlarmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.62
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on BITS 2 reference cleared
Cause	Generated when an alarm condition on the BITS 2 timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.103 tmnxEqSyncIfTimingBITS2Quality

Table 239: tmnxEqSyncIfTimingBITS2Quality properties

Property name	Value
Application name	CHASSIS
Event ID	2071
Event name	tmnxEqSyncIfTimingBITS2Quality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.59
Default severity	minor
Message format string	Synchronous Timing interface, reference BITS2 received quality level *$tmnxSyncIfTimingBITS2RxQltyLevel$*
Cause	Generated when there is a change of the received quality level on the second bits interface.
Effect	N/A
Recovery	N/A

9.104 tmnxEqSyncIfTimingBITSAlarm

Table 240: tmnxEqSyncIfTimingBITSAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2030
Event name	tmnxEqSyncIfTimingBITSAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.38
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on BITS*$bits-two-supported$* reference
Cause	Generated when an alarm condition on the BITS timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.105 tmnxEqSyncIfTimingBITSAlarmClear

Table 241: tmnxEqSyncIfTimingBITSAlarmClear properties

Property name	Value
Application name	CHASSIS
Event ID	2031
Event name	tmnxEqSyncIfTimingBITSAlarmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.39
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on BITS*$bits-two-supported$* reference cleared
Cause	Generated when an alarm condition on the BITS timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.106 tmnxEqSyncIfTimingBITSOutRefChg

Table 242: tmnxEqSyncIfTimingBITSOutRefChg properties

Property name	Value
Application name	CHASSIS
Event ID	2075
Event name	tmnxEqSyncIfTimingBITSOutRefChg
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.63
Default severity	minor
Message format string	Synchronous Timing interface, BITS output timing reference changed to *$tmnxSyncIfTimingBITSOutRefSel$*
Cause	Generated when the BITS Out timing reference selection changes.
Effect	N/A

Property name	Value
Recovery	N/A

9.107 tmnxEqSyncIfTimingBITSQuality

Table 243: tmnxEqSyncIfTimingBITSQuality properties

Property name	Value
Application name	CHASSIS
Event ID	2070
Event name	tmnxEqSyncIfTimingBITSQuality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.58
Default severity	minor
Message format string	Synchronous Timing interface, reference BITS *$bits-two-supported$* received quality level *$tmnxSyncIfTimingBITSRxQltyLevel$*
Cause	Generated when there is a change of the received quality level on the bits interface.
Effect	N/A
Recovery	N/A

9.108 tmnxEqSyncIfTimingHoldover

Table 244: tmnxEqSyncIfTimingHoldover properties

Property name	Value
Application name	CHASSIS
Event ID	2017
Event name	tmnxEqSyncIfTimingHoldover
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.26
Default severity	critical
Message format string	Synchronous Timing interface in holdover state

Property name	Value
Cause	Generated when the synchronous equipment timing subsystem transitions into a holdover state. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.109 tmnxEqSyncIfTimingHoldoverClear

Table 245: tmnxEqSyncIfTimingHoldoverClear properties

Property name	Value
Application name	CHASSIS
Event ID	2018
Event name	tmnxEqSyncIfTimingHoldoverClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.27
Default severity	critical
Message format string	Synchronous Timing interface holdover state cleared
Cause	Generated when the synchronous equipment timing subsystem transitions out of the holdover state. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.110 tmnxEqSyncIfTimingPTPAlarm

Table 246: tmnxEqSyncIfTimingPTPAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2080
Event name	tmnxEqSyncIfTimingPTPAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.68

Property name	Value
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on PTP reference
Cause	Generated when an alarm condition on the Precision Timing Protocol (PTP) timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.111 tmnxEqSyncIfTimingPTPAlarmClr

Table 247: tmnxEqSyncIfTimingPTPAlarmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2081
Event name	tmnxEqSyncIfTimingPTPAlarmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.69
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on PTP reference cleared
Cause	Generated when an alarm condition on the Precision Timing Protocol (PTP) timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.112 tmnxEqSyncIfTimingPTPQuality

Table 248: tmnxEqSyncIfTimingPTPQuality properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2079
Event name	tmnxEqSyncIfTimingPTPQuality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.67
Default severity	minor
Message format string	Synchronous Timing interface, reference PTP received quality level *$tmnxSyncIfTimingPTPRxQltyLevel$*
Cause	Generated when there is a change of the received quality level on the Precision Timing Protocol (PTP).
Effect	N/A
Recovery	N/A

9.113 tmnxEqSyncIfTimingRef1Alarm

Table 249: tmnxEqSyncIfTimingRef1Alarm properties

Property name	Value
Application name	CHASSIS
Event ID	2019
Event name	tmnxEqSyncIfTimingRef1Alarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.28
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on reference 1
Cause	Generated when an alarm condition on the first timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.114 tmnxEqSyncIfTimingRef1AlarmClear

Table 250: tmnxEqSyncIfTimingRef1AlarmClear properties

Property name	Value
Application name	CHASSIS
Event ID	2020
Event name	tmnxEqSyncIfTimingRef1AlarmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.29
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on reference 1 cleared
Cause	Generated when an alarm condition on the first timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.115 tmnxEqSyncIfTimingRef1Quality

Table 251: tmnxEqSyncIfTimingRef1Quality properties

Property name	Value
Application name	CHASSIS
Event ID	2068
Event name	tmnxEqSyncIfTimingRef1Quality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.56
Default severity	minor
Message format string	Synchronous Timing interface, reference 1 received quality level *$tmnxSyncIfTimingRef1RxQltyLevel$*
Cause	Generated when there is a change of the received quality level on timing reference 1.
Effect	N/A
Recovery	N/A

9.116 tmnxEqSyncIfTimingRef2Alarm

Table 252: tmnxEqSyncIfTimingRef2Alarm properties

Property name	Value
Application name	CHASSIS
Event ID	2021
Event name	tmnxEqSyncIfTimingRef2Alarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.30
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on reference 2
Cause	Generated when an alarm condition on the second timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

9.117 tmnxEqSyncIfTimingRef2AlarmClear

Table 253: tmnxEqSyncIfTimingRef2AlarmClear properties

Property name	Value
Application name	CHASSIS
Event ID	2022
Event name	tmnxEqSyncIfTimingRef2AlarmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.31
Default severity	minor
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on reference 2 cleared
Cause	Generated when an alarm condition on the second timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.

Property name	Value
Effect	N/A
Recovery	N/A

9.118 tmnxEqSyncIfTimingRef2Quality

Table 254: tmnxEqSyncIfTimingRef2Quality properties

Property name	Value
Application name	CHASSIS
Event ID	2069
Event name	tmnxEqSyncIfTimingRef2Quality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.57
Default severity	minor
Message format string	Synchronous Timing interface, reference 2 received quality level *$tmnxSyncIfTimingRef2RxQltyLevel$*
Cause	Generated when there is a change of the received quality level on timing reference 2.
Effect	N/A
Recovery	N/A

9.119 tmnxEqSyncIfTimingRefSwitch

Table 255: tmnxEqSyncIfTimingRefSwitch properties

Property name	Value
Application name	CHASSIS
Event ID	2072
Event name	tmnxEqSyncIfTimingRefSwitch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.60
Default severity	minor

Property name	Value
Message format string	Synchronous Timing interface, timing reference changed to *$tmnxSyncIfTimingRef1InUse$*
Cause	Generated when there is a change of which timing reference is providing timing for the system.
Effect	N/A
Recovery	N/A

9.120 tmnxEqSyncIfTimingSystemQuality

Table 256: tmnxEqSyncIfTimingSystemQuality properties

Property name	Value
Application name	CHASSIS
Event ID	2077
Event name	tmnxEqSyncIfTimingSystemQuality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.65
Default severity	minor
Message format string	Synchronous Timing interface, System Quality Level changed to *$tmnxSyncIfTimingSystemQltyLevel$*
Cause	This notification may be triggered for the following reasons: 1) There has been a switch in the timing reference in use by the network element, either because the previously active timing reference was disqualified, or to ensure that the network element is using the timing reference with the best timing quality. 2) There has been a change in the active timing reference's quality and the change does not result in a timing reference switch. 3) The network element has transitioned into or out of the holdover state.
Effect	The system quality level is used to determine the SSM code transmitted on synchronous interfaces. This may affect the SSM code transmitted on some or all interfaces, which may affect the distribution of timing throughout the network.
Recovery	If the customer is expecting the system to be locked to a reference of a particular quality and the system quality has decreased, the customer will need to determine the root cause (for example, loss of communication with a satellite) and resolve the issue.

9.121 tmnxEqWrongCard

Table 257: tmnxEqWrongCard properties

Property name	Value
Application name	CHASSIS
Event ID	2004
Event name	tmnxEqWrongCard
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.10
Default severity	minor
Message format string	Class *$tmnxHwClass$* : wrong type inserted
Cause	Generated when the wrong type of card is inserted into a slot of the chassis. Even though a card may be physically supported by the slot, it may have been administratively configured to allow only certain card types in a particular slot location. The card type may be IOM, Fabric, MDA, MCM, CPM module, etc.
Effect	N/A
Recovery	N/A

9.122 tmnxExtStandbyCpmReboot

Table 258: tmnxExtStandbyCpmReboot properties

Property name	Value
Application name	CHASSIS
Event ID	2127
Event name	tmnxExtStandbyCpmReboot
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.114
Default severity	warning
Message format string	Rebooting extension standby CPM due to master standby CPM reboot and transition into or out of an ISSU state.
Cause	The tmnxExtStandbyCpmReboot notification is generated after a master standby CPM reboots and it is determined that the master standby CPM has transitioned into or out of an ISSU state. This

Property name	Value
	detected transition will cause a reboot of the extension standby CPM (this reboot is necessary and expected for ISSU operation). This notification helps an operator understand why an extension standby CPM may have rebooted.
Effect	The extension standby CPM will reboot.
Recovery	There is no recovery for this notification.

9.123 tmnxExtStandbyCpmRebootFail

Table 259: tmnxExtStandbyCpmRebootFail properties

Property name	Value
Application name	CHASSIS
Event ID	2128
Event name	tmnxExtStandbyCpmRebootFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.115
Default severity	minor
Message format string	Unable to automatically reboot extension standby CPM during ISSU.
Cause	The tmnxExtStandbyCpmRebootFail notification is generated after a master standby CPM reboots and it is determined that the master standby CPM has transitioned into or out of an ISSU state. The system will attempt to reboot the extension standby CPM as part of the normal ISSU process. If the system determines that it cannot reboot the extension standby CPM (i.e. it is not reachable) then this log event is raised.
Effect	The extension standby CPM may not transition to the ISSU state in which case the ISSU cannot proceed normally.
Recovery	Resetting the extension standby CPM can be attempted to try and get the CPM into an ISSU state. If that is not successful, then the ISSU should be aborted.

9.124 tmnxInterChassisCommsDown

Table 260: tmnxInterChassisCommsDown properties

Property name	Value
Application name	CHASSIS
Event ID	4001
Event name	tmnxInterChassisCommsDown
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxInterChassis Notifications.1
Default severity	critical
Message format string	Control communications disrupted between the active CPM and the chassis
Cause	The tmnxInterChassisCommsDown alarm is generated when the active CPM cannot reach the far-end chassis.
Effect	The resources on the far-end chassis are not available. This event for the far-end chassis means that the CPM, SFM, and XCM cards in the far-end chassis will reboot and remain operationally down until communications are re-established.
Recovery	Ensure that all CPM interconnect ports in the system are properly cabled together with working cables.

9.125 tmnxInterChassisCommsUp

Table 261: tmnxInterChassisCommsUp properties

Property name	Value
Application name	CHASSIS
Event ID	4002
Event name	tmnxInterChassisCommsUp
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxInterChassis Notifications.2
Default severity	critical
Message format string	Control communications established between the active CPM and the chassis

Property name	Value
Cause	The tmnxInterChassisCommsUp notification is generated when the control communications are re-established between the active CPM and the far-end chassis.
Effect	The resources on the far-end chassis are now available. This event for the far-end chassis means that the CPM, SFM and XCM cards in the far-end chassis will start the process of coming back into service.
Recovery	N/A

9.126 tmnxIomEventOverflow

Table 262: tmnxIomEventOverflow properties

Property name	Value
Application name	CHASSIS
Event ID	2124
Event name	tmnxIomEventOverflow
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.111
Default severity	minor
Message format string	Iom *$tmnxIomResourceType$* Resource event overflow occurred on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxIomResLimitTime EventOccured$*.
Cause	The tmnxIomEventOverflow notification is generated when tmnx IomResStateClr, tmnxIomResExhausted and tmnxIomResHighLimit Reached occur more than 200 times because of resource usage fluctuation. The Iom Raises the final trap to indicate overflow and stops logging traps.
Effect	Some FP notifications configured on the card may not be received.
Recovery	Notifications will resume once the Overflow clear is set.

9.127 tmnxIomEventOverflowClr

Table 263: tmnxIomEventOverflowClr properties

Property name	Value
Application name	CHASSIS
Event ID	2125
Event name	tmnxIomEventOverflowClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.112
Default severity	minor
Message format string	*$tmnxIomResLimMissingNotifCount$* Iom *$tmnxIomResourceType $* Resources events were dropped in the last event throttling interval on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxIomResLimitTime EventOccured$*.
Cause	The tmnxIomEventOverflowClr notification is generated when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

9.128 tmnxIomResExhausted

Table 264: tmnxIomResExhausted properties

Property name	Value
Application name	CHASSIS
Event ID	2122
Event name	tmnxIomResExhausted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.109
Default severity	critical
Message format string	The *$tmnxIomResourceType$* resources on IOM *$tmnxChassisNotify CardSlotNum$* and Forwarding Plane *$tmnxChassisNotifyFpNum$* has been exhausted at *$tmnxIomResLimitTimeEventOccured$*.

Property name	Value
Cause	The tmnxIomResExhausted notification is generated when the type of resources on IOM as specified by tmnxIomResourceType has reached the 100% of its utilization threshold.
Effect	The specified resource has reached the stats pool limit.
Recovery	Intervention may be required to recover resources.

9.129 tmnxIomResHighLimitReached

Table 265: tmnxIomResHighLimitReached properties

Property name	Value
Application name	CHASSIS
Event ID	2121
Event name	tmnxIomResHighLimitReached
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.108
Default severity	major
Message format string	The *$tmnxIomResourceType$* resources on IOM *$tmnxChassisNotifyCardSlotNum$* and Forwarding Plane *$tmnxChassisNotifyFpNum$* has reached the *$tmnxIomResourceLimitPct$*% utilization threshold at *$tmnxIomResLimitTimeEventOccured$*.
Cause	The tmnxIomResHighLimitReached notification is generated when the resource (of type tmnxIomResourceType) utilization on IOM has reached the value of tmnxIomResourceLimitPct.
Effect	The specified resource limit is cleared when the number of in-use stats resources falls below the clear threshold of the stats pool limit.
Recovery	There is no recovery required for this notification.

9.130 tmnxIomResStateClr

Table 266: tmnxIomResStateClr properties

Property name	Value
Application name	CHASSIS
Event ID	2123

Property name	Value
Event name	tmnxIomResStateClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.110
Default severity	minor
Message format string	The *$tmnxIomResourceType$* resources on IOM *$tmnxChassisNotifyCardSlotNum$* and Forwarding Plane *$tmnxChassisNotifyFpNum$* has dropped below the *$tmnxIomResourceLimitPct$*% utilization threshold at *$tmnxIomResLimitTimeEventOccured$*.
Cause	The tmnxIomResStateClr notification is generated when the type of resources on IOM as specified by tmnxIomResourceType has dropped back down below the value of tmnxIomResourceLimitPct.
Effect	The specified resource limit is cleared when the number of in-use stats resources falls below tmnxIomResourceLimitPct of the stats pool limit.
Recovery	There is no recovery required for this notification.

9.131 tmnxIPsecIsaGrpActiveIsaChgd

Table 267: tmnxIPsecIsaGrpActiveIsaChgd properties

Property name	Value
Application name	CHASSIS
Event ID	2062
Event name	tmnxIPsecIsaGrpActiveIsaChgd
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.50
Default severity	minor
Message format string	Active ISA changed to *$tmnxIPsecIsaGrpActiveIsa$* for IPSec ISA group *$tmnxIPsecIsaGrpId$* where primary ISA is *$tmnxIPsecIsaGrpPrimaryIsa$* and Backup ISA is *$tmnxIPsecIsaGrpBackupIsa$*
Cause	The tmnxIPsecIsaGrpActiveIsaChgd notification is generated when a change in the active ISA (Integrated Service Adaptor) occurs in an IPsec ISA module group.
Effect	N/A
Recovery	N/A

9.132 tmnxIPsecIsaGrpTnlHighWMark

Table 268: tmnxIPsecIsaGrpTnlHighWMark properties

Property name	Value
Application name	CHASSIS
Event ID	2066
Event name	tmnxIPsecIsaGrpTnlHighWMark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.54
Default severity	minor
Message format string	Number of tunnels for an IPsec ISA module for the group *$tmnxIPsecIsaGrpId$* has reached to the high watermark which is 95% of the maximum limit *$tmnxIPsecIsaGrpMaxTunnels$*.
Cause	The number of tunnels for an IPsec ISA (Integrated Service Adaptor) module has reached to the high watermark which is 95% of the maximum limit.
Effect	N/A
Recovery	N/A

9.133 tmnxIPsecIsaGrpTnlLowWMark

Table 269: tmnxIPsecIsaGrpTnlLowWMark properties

Property name	Value
Application name	CHASSIS
Event ID	2065
Event name	tmnxIPsecIsaGrpTnlLowWMark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.53
Default severity	minor
Message format string	Number of tunnels for an IPsec ISA module for the group *$tmnxIPsecIsaGrpId$* has dropped to the low watermark which is 90% of the maximum limit *$tmnxIPsecIsaGrpMaxTunnels$*.
Cause	The number of tunnels for an IPsec ISA (Integrated Service Adaptor) module has dropped to the low watermark which is 90% of the maximum limit.

Property name	Value
Effect	N/A
Recovery	N/A

9.134 tmnxIPsecIsaGrpTnlMax

Table 270: tmnxIPsecIsaGrpTnlMax properties

Property name	Value
Application name	CHASSIS
Event ID	2067
Event name	tmnxIPsecIsaGrpTnlMax
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.55
Default severity	minor
Message format string	Number of tunnels for an IPsec ISA module the for group *$tmnxIPsec IsaGrpId$* has reached the maximum limit *$tmnxIPsecIsaGrpMax Tunnels$*.
Cause	The number of tunnels for an IPsec ISA (Integrated Service Adaptor) module has reached the maximum limit.
Effect	N/A
Recovery	N/A

9.135 tmnxIPsecIsaGrpUnableToSwitch

Table 271: tmnxIPsecIsaGrpUnableToSwitch properties

Property name	Value
Application name	CHASSIS
Event ID	2064
Event name	tmnxIPsecIsaGrpUnableToSwitch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.52
Default severity	minor

Property name	Value
Message format string	IPsec ISA *$tmnxIPsecIsaGrpActiveIsa$* for group *$tmnxIPsecIsaGrpId $* is unable to switch due to lack of resources on the destination MDA
Cause	IPsec ISA group is unable to switch due to lack of resources on the destination MDA.
Effect	In such an event the IPsec ISA group is left without an active MDA and the tmnxIPsecIsaGrpOperState is set to 'outOfService'.
Recovery	Recovery is possible by releasing resources and performing a shutdown/no shutdown operation to bring up the ISA group.

9.136 tmnxMDAIsaTunnelGroupChange

Table 272: tmnxMDAIsaTunnelGroupChange properties

Property name	Value
Application name	CHASSIS
Event ID	2083
Event name	tmnxMDAIsaTunnelGroupChange
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.71
Default severity	minor
Message format string	MDA *$tmnxCardSlotNum$*/ *$tmnxMDASlotNum$* is *$tmnxMDAIsa TunnelGroupInUse$* active in the ISA tunnel-group *$tmnxMDAIsa TunnelGroup$*
Cause	The tmnxMDAIsaTunnelGroupChange notification is generated when IPsec ISA (Integrated Service Adaptor) tunnel-group in-use for the MDA changes value.
Effect	There is no operational impact due to this event.
Recovery	N/A

9.137 tmnxOesCardDegraded

Table 273: tmnxOesCardDegraded properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	5123
Event name	tmnxOesCardDegraded
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.23
Default severity	minor
Message format string	Class *$tmnxHwClass$*: Card degraded
Cause	The tmnxOesCardDegraded notification is generated when a fault on the card has caused the system to declare a hardware failure. This condition may be declared due to a failure in the SEEP or another hardware failure, depending on the card type the alarm is raised against.
Effect	The tmnxOesCardDegraded alarm indicates a lower priority fault on the card that does not directly affect the traffic currently flowing through the device.
Recovery	First attempt a soft reset of the card. If the card has rebooted and the condition did not clear, then try a hard reset of the card. If the card has rebooted and the condition did not clear, then remove the card and re-insert it to see if the condition clears. If the condition remains, then replace the card and follow the return and repair process for the problem card.

9.138 tmnxOesCardFirmwareErr

Table 274: tmnxOesCardFirmwareErr properties

Property name	Value
Application name	CHASSIS
Event ID	5132
Event name	tmnxOesCardFirmwareErr
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.33
Default severity	minor
Message format string	Class *$tmnxHwClass$*: Inventory error
Cause	The tmnxOesCardFirmwareErr is raised when the device installed in the shelf has an EEPROM that does not contain the correct or recognizable information.

Property name	Value
Effect	The card may demonstrate other alarms due to this condition.
Recovery	Replace the card.

9.139 tmnxOesCfgBlocked

Table 275: tmnxOesCfgBlocked properties

Property name	Value
Application name	CHASSIS
Event ID	5139
Event name	tmnxOesCfgBlocked
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.15
Default severity	minor
Message format string	OES Configuration blocked
Cause	This event tmnxOesCfgBlocked notification is generated when a configuration being made in the OES is blocked.
Effect	The configuration is not active in the OES.
Recovery	One possible reason for this configuration failure is if there is a card present in the OES that is a supported card type but the router was not yet aware of its presence. This condition should clear as soon as the router becomes aware of the card. A second reason is when the supported card is present and is misaligned with the configuration (e.g. card present in slot 3 and 4, yet configuration is oes-1/2 where the width of card is two slots). This condition cannot be cleared automatically as the card has to be moved to the correct slot (or the configuration has to be removed for card oes-1/3 via cli command). A third reason is when there is an unsupported card type in the OES that the router cannot manage. This condition cannot be cleared automatically and the OES will need to be recommissioned to clear the condition. Note: services on cards not impacted by the unknown card type are not affected.

9.140 tmnxOesCfgFailNoMemory

Table 276: tmnxOesCfgFailNoMemory properties

Property name	Value
Application name	CHASSIS
Event ID	5138
Event name	tmnxOesCfgFailNoMemory
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.14
Default severity	minor
Message format string	OES Configuration failed due to insufficient dynamic memory
Cause	The tmnxOesCfgFailNoMemory notification is generated when a request to obtain dynamic memory to download a configuration to the OES has failed.
Effect	The configuration is not active in the OES.
Recovery	This may be a temporary issue and the condition may clear on its own. If the event is raised periodically, then there is a permanent memory issue and the support organization should be informed.

9.141 tmnxOesCtlCardActivityChange

Table 277: tmnxOesCtlCardActivityChange properties

Property name	Value
Application name	CHASSIS
Event ID	5117
Event name	tmnxOesCtlCardActivityChange
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.17
Default severity	minor
Message format string	OES active control card changed to *$tmnxHwIndex$*
Cause	The tmnxOesCtlCardActivityChange notification is generated when the active Equipment Controller has changed to the card specified by the tmnxHwIndex.
Effect	The active Equipment Controller has moved to the previously standby card.

Property name	Value
Recovery	No recovery is required.

9.142 tmnxOesCtlCardPortDown

Table 278: tmnxOesCtlCardPortDown properties

Property name	Value
Application name	CHASSIS
Event ID	5101
Event name	tmnxOesCtlCardPortDown
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.1
Default severity	minor
Message format string	OES Ctl Card Port is not operational
Cause	The tmnxOesCtlCardPortDown notification is generated when a port (e.g. ES 1 or AUX) on an OES Control Card (e.g. EC card) is not operational. The reason may be a misconnected, disconnected or faulty cable, a faulty port or Control Card.
Effect	If an ES (Extension Shelf) port is down then one of the control plane communication paths between EC (Equipment Controller) cards in different OES Chassis is not available. The control communications with one or more OES subtending chassis may be affected rendering the Chassis unmanageable. Other control paths may be available. If an AUX port is down then one of the control plane communication paths between the router and the OES Master Chassis is not available and control communications with the OES may be affected rendering the OES unmanageable. Other control paths may be available.
Recovery	Check that the cable is correctly connected and test the cable.

9.143 tmnxOesCtlCardPortUp

Table 279: tmnxOesCtlCardPortUp properties

Property name	Value
Application name	CHASSIS
Event ID	5102

Property name	Value
Event name	tmnxOesCtlCardPortUp
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.2
Default severity	minor
Message format string	OES Ctl Card Port is operational
Cause	The tmnxOesCtlCardPortUp notification is generated when the port on the OES Control Card (e.g. EC card) is operational.
Effect	If an ES port is up then a control plane communication path between EC cards in different OES Chassis has been established. If an AUX port is up then a control plane communication path between the router and the OES Master Chassis has been established and the OES can be managed by the router.
Recovery	No recovery required

9.144 tmnxOesCtlCommsDown

Table 280: tmnxOesCtlCommsDown properties

Property name	Value
Application name	CHASSIS
Event ID	5001
Event name	tmnxOesCtlCommsDown
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.1
Default severity	critical
Message format string	Control communications disrupted between the Active CPM and the OES Master chassis, reason: *$tmnxOesCtlCommsDownReason$*
Cause	The tmnxOesCtlCommsDown notification is generated when the active CPM can't reach the OES master chassis.
Effect	The OES can't be managed by the router.
Recovery	Ensure that all control communications ports between the router and the OES master chassis are correctly connected and test the cables.

9.145 tmnxOesCtlCommsUp

Table 281: tmnxOesCtlCommsUp properties

Property name	Value
Application name	CHASSIS
Event ID	5002
Event name	tmnxOesCtlCommsUp
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.2
Default severity	critical
Message format string	Control communications established between the Active CPM and the OES Master chassis
Cause	The tmnxOesCtlCommsUp notification is generated when the active CPM can reach the OES master chassis.
Effect	The OES can be managed by the router.
Recovery	No recovery required.

9.146 tmnxOesDbInvalid

Table 282: tmnxOesDbInvalid properties

Property name	Value
Application name	CHASSIS
Event ID	5005
Event name	tmnxOesDbInvalid
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.5
Default severity	major
Message format string	OES database invalid
Cause	The tmnxOesDbInvalid notification may be raised under the following conditions: 1) During initial installation, if the OES is not properly commissioned. 2) The serial number in the database does not match that of the OES either because the controller was replaced or the alarm card was replaced. 3) A downgrade of OES software has occurred. 4) Equipment Controller is removed/reseated during a system process,

Property name	Value
	causing file corruption. 5) The database audit failed indicating some type of corruption of the database.
Effect	The OES is not in a normal operating mode. It does not have the correct configuration and the state of its cards is unpredictable. As a result, the OES will not boot normally and not all commands are allowed.
Recovery	A database corruption on the OES requires that the OES be re-commissioned. The correct database is held in the host system so it will be restored to the shelf once the existing database is cleared and the host re-establishes communication with the OES.

9.147 tmnxOesDbInvalidClear

Table 283: tmnxOesDbInvalidClear properties

Property name	Value
Application name	CHASSIS
Event ID	5006
Event name	tmnxOesDbInvalidClear
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.6
Default severity	major
Message format string	OES database invalid cleared
Cause	The tmnxOesDbInvalidClear notification is generated when the active Equipment Controller previously under tmnxOesDbInvalid condition now contains a valid database.
Effect	The OES active Equipment Controller's database is now valid.
Recovery	No recovery is required.

9.148 tmnxOesDbSyncFailure

Table 284: tmnxOesDbSyncFailure properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	5003
Event name	tmnxOesDbSyncFailure
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.3
Default severity	minor
Message format string	OES database synchronization failure
Cause	The tmnxOesDbSyncFailure notification may be raised under the following conditions: 1) An incorrectly seated Equipment Controller. 2) The software versions on the active and inactive Equipment Controllers are not compatible. 3) A hardware problem with one or both controllers.
Effect	The OES does not have redundancy protection between the two Equipment Controller cards.
Recovery	Proceed as follows to clear the Database Synchronization Failed alarm: 1) Remove the Equipment Controller with the condition and examine the connector on the back of the card for damage, including bent or broken pins. 2) Examine the connector on the backplane for damage. If there is damage to the backplane of the shelf, contact your service representative. 3) Re-insert the Equipment Controller into its original slot and allow the card to initialize. 4) Repeat Step 2) through Step 4) for the second Equipment Controller. 5) Replace the Equipment Controller with the alarm condition with a new unit. If the condition is not cleared, replace the second Equipment Controller with a new unit. Follow the return and repair process to return the faulty card to an authorized repair center for replacement.

9.149 tmnxOesDbSyncFailureClear

Table 285: tmnxOesDbSyncFailureClear properties

Property name	Value
Application name	CHASSIS
Event ID	5004
Event name	tmnxOesDbSyncFailureClear
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.4
Default severity	minor
Message format string	OES database synchronization failure cleared

Property name	Value
Cause	The tmnxOesDbSyncFailureClear notification is generated when the active Equipment Controller is able to synchronize its database with the inactive Equipment Controller.
Effect	The active and inactive Equipment Controller's databases are now synchronized.
Recovery	No recovery required.

9.150 tmnxOesDbUnsync

Table 286: tmnxOesDbUnsync properties

Property name	Value
Application name	CHASSIS
Event ID	5007
Event name	tmnxOesDbUnsync
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.7
Default severity	minor
Message format string	OES active and standby EC databases out of sync
Cause	The tmnxOesDbUnsync notification is generated when the active and standby Equipment Controllers are not in sync.
Effect	The OES does not have redundancy protection between the two Equipment Controller cards. If a switchover were to occur, then the database of the newly active controller might not reflect the latest configuration.
Recovery	Proceed as follows to clear the Database Unsynchronization alarm: 1) Perform a warm reset of the standby controller; 2) If step 1 does not clear the alarm condition, then contact the next level of technical support for help.

9.151 tmnxOesDbUnsyncClear

Table 287: tmnxOesDbUnsyncClear properties

Property name	Value
Application name	CHASSIS
Event ID	5008
Event name	tmnxOesDbUnsyncClear
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.8
Default severity	minor
Message format string	OES active and standby EC databases synchronized
Cause	The tmnxOesDbUnsyncClear notification is generated when the previously out of sync database is now synchronized between the active and standby Equipment Controller cards.
Effect	The database is synchronized between the active and standby Equipment Controller cards.
Recovery	No recovery is required.

9.152 tmnxOesFan32HReqd

Table 288: tmnxOesFan32HReqd properties

Property name	Value
Application name	CHASSIS
Event ID	5107
Event name	tmnxOesFan32HReqd
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.7
Default severity	critical
Message format string	OES high speed fan required (FAN32H)
Cause	The tmnxOesFan32HReqd notification is generated when the OES chassis requires high speed fan (FAN32H), but the fan inserted is not FAN32H type.
Effect	The OES chassis is not operating with required fan type.
Recovery	Replace the OES fan unit with FAN32H.

9.153 tmnxOesFan32HReqdClear

Table 289: tmnxOesFan32HReqdClear properties

Property name	Value
Application name	CHASSIS
Event ID	5108
Event name	tmnxOesFan32HReqdClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.8
Default severity	critical
Message format string	Cleared: OES high speed fan required (FAN32H)
Cause	The tmnxOesFan32HReqdClear notification is generated when the OES chassis is equipped with FAN32H or when the alarmed fan unit with tmnxOesFan32HReqd condition is removed from the slot.
Effect	The OES chassis is operating with required FAN32H type, or the incorrect fan unit has been removed.
Recovery	No recovery required.

9.154 tmnxOesFanFailure

Table 290: tmnxOesFanFailure properties

Property name	Value
Application name	CHASSIS
Event ID	5109
Event name	tmnxOesFanFailure
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.9
Default severity	critical
Message format string	OES Fan Failure: *$tmnxOesNotifyFailureReason$*
Cause	The tmnxOesFanFailure notification is generated when the fan unit in an OES chassis has failed. tmnxOesNotifyFailureReason contains the reason for fan failure.
Effect	The fan unit in the OES chassis is out of service.

Property name	Value
Recovery	If the condition causing fan failure can not be removed, replace the faulty fan unit.

9.155 tmnxOesFanFailureClear

Table 291: tmnxOesFanFailureClear properties

Property name	Value
Application name	CHASSIS
Event ID	5110
Event name	tmnxOesFanFailureClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.10
Default severity	critical
Message format string	Clear OES Fan Failure: *$tmnxOesNotifyFailureReason$*
Cause	The tmnxOesFanFailureClear notification is generated when fan failure in an OES chassis is cleared. tmnxOesNotifyFailureReason contains the reason for fan failure being cleared.
Effect	The fan unit in the OES chassis is in service.
Recovery	No recovery required.

9.156 tmnxOesFanInserted

Table 292: tmnxOesFanInserted properties

Property name	Value
Application name	CHASSIS
Event ID	5106
Event name	tmnxOesFanInserted
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.6
Default severity	critical
Message format string	OES Fan Inserted

Property name	Value
Cause	The tmnxOesFanInserted notification is generated when the OES fan unit is inserted into its slot in the OES chassis.
Effect	The OES chassis is now equipped with a fan unit.
Recovery	No recovery required.

9.157 tmnxOesFanRemoved

Table 293: tmnxOesFanRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	5105
Event name	tmnxOesFanRemoved
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.5
Default severity	critical
Message format string	OES Fan Removed
Cause	The tmnxOesFanRemoved notification is generated when the OES fan unit is removed from its slot in the OES chassis.
Effect	The function of OES fan unit is not available.
Recovery	Insert OES fan unit into its slot.

9.158 tmnxOesFanSpeedHigh

Table 294: tmnxOesFanSpeedHigh properties

Property name	Value
Application name	CHASSIS
Event ID	5124
Event name	tmnxOesFanSpeedHigh
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.24
Default severity	minor

Property name	Value
Message format string	OES Fan speed is too high
Cause	The tmnxOesFanSpeedHigh notification is generated when the fan speed is too high, based upon the current shelf cooling requirements.
Effect	The fans run faster than required.
Recovery	Remove and re-insert the fan tray into the chassis. If the alarm does not clear then replace the fan tray.

9.159 tmnxOesFanSpeedHighClear

Table 295: tmnxOesFanSpeedHighClear properties

Property name	Value
Application name	CHASSIS
Event ID	5125
Event name	tmnxOesFanSpeedHighClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.25
Default severity	minor
Message format string	OES Fan speed is too high cleared
Cause	The tmnxOesFanSpeedHighClear notification is generated when the conditions causing a tmnxOesFanSpeedHigh notification have been cleared. Fan speed has returned to acceptable conditions.
Effect	The fan speed is normal.
Recovery	No recovery is required.

9.160 tmnxOesFanSpeedLow

Table 296: tmnxOesFanSpeedLow properties

Property name	Value
Application name	CHASSIS
Event ID	5126
Event name	tmnxOesFanSpeedLow

Property name	Value
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.26
Default severity	minor
Message format string	OES Fan speed is too low
Cause	The tmnxOesFanSpeedLow notification is generated when the fan speed is too low, based upon the current shelf cooling requirements.
Effect	The fans run slower than required.
Recovery	Check for airflow blockage or a dirty filter, and clear. If no problems are found, replace the fan tray.

9.161 tmnxOesFanSpeedLowClear

Table 297: tmnxOesFanSpeedLowClear properties

Property name	Value
Application name	CHASSIS
Event ID	5127
Event name	tmnxOesFanSpeedLowClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.27
Default severity	minor
Message format string	OES Fan speed is too low cleared
Cause	The tmnxOesFanSpeedLowClear notification is generated when the conditions causing a tmnxOesFanSpeedLow notification have been cleared. Fan speed has returned to acceptable conditions.
Effect	The fan speed is normal.
Recovery	No recovery is required.

9.162 tmnxOesFirmwareCondition

Table 298: tmnxOesFirmwareCondition properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	5137
Event name	tmnxOesFirmwareCondition
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.13
Default severity	minor
Message format string	Class *$tmnxHwClass$*: *$tmnxOesEventReason$*
Cause	The tmnxOesFirmwareCondition notification is generated when the firmware on the card has a condition that needs to be notified to network administrator. The value of tmnxOesEventReason object specifies the specific reason for the condition.
Effect	Not all the features may be available.
Recovery	Perform a hard reset of the card. If the condition persists, then contact Nokia customer support.

9.163 tmnxOesFpgaFail

Table 299: tmnxOesFpgaFail properties

Property name	Value
Application name	CHASSIS
Event ID	5118
Event name	tmnxOesFpgaFail
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.18
Default severity	critical
Message format string	OES FPGA download failure
Cause	The tmnxOesFpgaFail notification is generated during an out-of-service upgrade when the FPGA file downloaded to the card was corrupt or the FPGA failed to program correctly.
Effect	The OES card shall automatically cold reboot and the card shall attempt to recover. While the condition exists the card remains out-of-service.
Recovery	If the card has rebooted and the condition did not clear, then first reseat the card and see if the condition clears. If the condition remains, then replace the card and follow the return and repair process for the problem card.

9.164 tmnxOesFpgaFailClear

Table 300: tmnxOesFpgaFailClear properties

Property name	Value
Application name	CHASSIS
Event ID	5119
Event name	tmnxOesFpgaFailClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.19
Default severity	critical
Message format string	OES FPGA download failure cleared
Cause	The tmnxOesFpgaFailClear notification is generated when the FPGA is successfully programmed.
Effect	The FPGA is successfully programmed.
Recovery	No recovery is required.

9.165 tmnxOesFpgaTimeout

Table 301: tmnxOesFpgaTimeout properties

Property name	Value
Application name	CHASSIS
Event ID	5120
Event name	tmnxOesFpgaTimeout
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.20
Default severity	critical
Message format string	OES FPGA timeout
Cause	The tmnxOesFpgaTimeout notification is generated when the FPGA file download and reprogramming took longer than expected (about 45 minutes).
Effect	The FPGA on the indicated card was not reprogrammed in the time window.

Property name	Value
Recovery	If the OES card is operational, wait for a maintenance window and reset the OES card.

9.166 tmnxOesFpgaTimeoutClear

Table 302: tmnxOesFpgaTimeoutClear properties

Property name	Value
Application name	CHASSIS
Event ID	5121
Event name	tmnxOesFpgaTimeoutClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.21
Default severity	critical
Message format string	OES FPGA timeout cleared
Cause	The tmnxOesFpgaTimeoutClear notification is generated when the OES FPGA timeout condition is cleared.
Effect	The FPGA is successfully programmed.
Recovery	No recovery is required.

9.167 tmnxOesNtpOutOfSync

Table 303: tmnxOesNtpOutOfSync properties

Property name	Value
Application name	CHASSIS
Event ID	5134
Event name	tmnxOesNtpOutOfSync
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.10
Default severity	minor
Message format string	NTP is enabled but not in sync with NTP server
Cause	The tmnxOesNtpOutOfSync notification is generated when NTP time on the OES is not synchronized to the host router. The host router

Property name	Value
	must have NTP enabled and have recovered time from external time sources (NTP to PTP). If there is no NTP time source for the router, it will not serve time to the OES. In addition, once the NE is power cycled, it takes approximately 20-30 minutes to initialize. Thereafter, time synchronization will be completed, with a maximum delay time of 2-3 minutes.
Effect	Timestamp of event occurring on the OES may not be exactly aligned with the host router.
Recovery	Ensure the host router has NTP configured and a reachable time source. Allow 40 minutes for the condition to clear.

9.168 tmnxOesNtpSync

Table 304: tmnxOesNtpSync properties

Property name	Value
Application name	CHASSIS
Event ID	5135
Event name	tmnxOesNtpSync
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.11
Default severity	minor
Message format string	NTP is enabled but not in sync with NTP server cleared
Cause	The tmnxOesNtpSync notification is generated when NTP on the OES is synchronized to the host router. The host router is serving acceptable time toward the OES and the OES has completed initial acquisition of time from the host.
Effect	None.
Recovery	No recovery is required.

9.169 tmnxOesOptTrnspndrMiscFail

Table 305: tmnxOesOptTrnspndrMiscFail properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	5122
Event name	tmnxOesOptTrnspndrMiscFail
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.22
Default severity	minor
Message format string	Class *$tmnxHwClass$*: miscellaneous failure
Cause	The tmnxOesOptTrnspndrMiscFail notification is generated when a non-service affecting hardware defect is detected on the card. This condition may be declared on the card due to one of the following causes: 1) Detection of line side transmitter laser bias or optical output power nearing end-of-life. 2) Detection of line receiver ITLA (Integrated Tunable Laser Assembly) laser bias or output power nearing end-of-life. 3) Detection of board-level Analog-to-Digital Conversion Digital Signal Processor (ADC DSP) device defect. 4) A device-to-device interface communication problem.
Effect	The tmnxOesOptTrnspndrMiscFail alarm indicates a lower priority fault on the card that does not directly affect the traffic currently flowing through the card. However, the card should be replaced at the next available maintenance opportunity.
Recovery	Replace the card.

9.170 tmnxOesPowerSupplyFailure

Table 306: tmnxOesPowerSupplyFailure properties

Property name	Value
Application name	CHASSIS
Event ID	5113
Event name	tmnxOesPowerSupplyFailure
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.13
Default severity	critical
Message format string	OES Power Supply Failure: *$tmnxOesNotifyFailureReason$*
Cause	The tmnxOesPowerSupplyFailure notification is generated when the power supply unit in the indicated slot of the OES chassis has failed. tmnxOesNotifyFailureReason contains the reason for the failure.

Property name	Value
Effect	The indicated OES power supply unit is out of service.
Recovery	If the condition causing the power supply failure can not be removed, replace the faulty power supply unit.

9.171 tmnxOesPowerSupplyFailureClear

Table 307: tmnxOesPowerSupplyFailureClear properties

Property name	Value
Application name	CHASSIS
Event ID	5114
Event name	tmnxOesPowerSupplyFailureClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.14
Default severity	critical
Message format string	Clear OES Power Supply Failure: *$tmnxOesNotifyFailureReason$*
Cause	The tmnxOesPowerSupplyFailureClear notification is generated when the power supply failure in the indicated slot of the OES chassis is cleared. tmnxOesNotifyFailureReason contains the reason for the power supply failure being cleared.
Effect	The indicated power supply unit in the OES chassis is in service.
Recovery	No recovery required.

9.172 tmnxOesPowerSupplyInserted

Table 308: tmnxOesPowerSupplyInserted properties

Property name	Value
Application name	CHASSIS
Event ID	5112
Event name	tmnxOesPowerSupplyInserted
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.12
Default severity	major

Property name	Value
Message format string	OES Power Supply Inserted
Cause	The tmnxOesPowerSupplyInserted notification is generated when the OES power supply unit is inserted into its slot in the OES chassis.
Effect	The indicated slot of the OES chassis is now equipped with the power supply unit.
Recovery	No recovery required.

9.173 tmnxOesPowerSupplyRemoved

Table 309: tmnxOesPowerSupplyRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	5111
Event name	tmnxOesPowerSupplyRemoved
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.11
Default severity	major
Message format string	OES Power Supply Removed
Cause	The tmnxOesPowerSupplyRemoved notification is generated when an OES power supply unit is removed from its slot in the OES chassis.
Effect	The power supply unit is not present in the indicated OES chassis slot.
Recovery	Insert OES power supply unit into its slot.

9.174 tmnxOesRedundancyFail

Table 310: tmnxOesRedundancyFail properties

Property name	Value
Application name	CHASSIS
Event ID	5130
Event name	tmnxOesRedundancyFail

Property name	Value
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.30
Default severity	minor
Message format string	Class *$tmnxHwClass$*: Equipment controller redundancy failure
Cause	The tmnxOesRedundancyFail notification is generated when the inactive equipment controller card in the OES is not providing redundancy protection. In some cases this is a transitory alarm that occurs as redundant Equipment Controllers discover one another and synchronize. Typical causes for the persistence of this alarm are: 1) Irreconcilable database schemas. 2) Inability to support system timing. 3) System timing is compromised. The inactive controller system timing module is not reporting the same status as the active controller or is reporting an error that the active controller does not have. 4) Subshelf link missing. Reasons that are generally transitory are: 1) Database not yet fully synchronized. 2) Software loads are not yet synchronized. Some or all of these may apply when the alarm is raised.
Effect	The OES is not protected against failure of the active Equipment Controller.
Recovery	Check for the Redundancy demerit in the detailed information of the chassis indicated.

9.175 tmnxOesRedundancyReady

Table 311: tmnxOesRedundancyReady properties

Property name	Value
Application name	CHASSIS
Event ID	5131
Event name	tmnxOesRedundancyReady
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.31
Default severity	minor
Message format string	Class *$tmnxHwClass$*: Redundancy ready
Cause	The tmnxOesRedundancyReady notification is generated when the equipment controller cards in the indicated OES chassis are providing redundant protection. The equipment controller cards are synchronized.
Effect	The equipment controller cards are synchronized.

Property name	Value
Recovery	No recovery is required.

9.176 tmnxOesSwBelowMinRev

Table 312: tmnxOesSwBelowMinRev properties

Property name	Value
Application name	CHASSIS
Event ID	5136
Event name	tmnxOesSwBelowMinRev
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.12
Default severity	minor
Message format string	OES running software version *$tmnxOesRunningSwImage$* is below the minimum expected version *$tmnxOesExpectedSwImage$*
Cause	The tmnxOesSwBelowMinRev notification is generated when the version of the running OES software image is below the minimum expected version.
Effect	The OES may not be operating as expected.
Recovery	Upgrade the OES to a software image that is equal to or greater than the minimum expected version.

9.177 tmnxOesSwUpgdCleanupFailed

Table 313: tmnxOesSwUpgdCleanupFailed properties

Property name	Value
Application name	CHASSIS
Event ID	5140
Event name	tmnxOesSwUpgdCleanupFailed
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.16
Default severity	minor

Property name	Value
Message format string	*$tmnxHwClass$* : Software upgrade cleanup failed: *$tmnxOesEvent Reason$*
Cause	This event tmnxOesSwUpgdCleanupFailed notification is generated when the operation to clean-up a failed software upgrade fails. The reason for the failure is specified in the object tmnxOesEventReason.
Effect	The OES software revision cannot be determined and so the operational state of the respective OES or OES card is indeterminate.
Recovery	1) Determine the reason for the upgrade failure from tmnxOes SwUpgradeCancelFlrReason in the notification. First clear the condition indicated by the reason. 2) Re-try the upgrade procedure. 3) Contact the Nokia technical support team if the re-try does not fix the problem.

9.178 tmnxOesSwUpgdFailed

Table 314: tmnxOesSwUpgdFailed properties

Property name	Value
Application name	CHASSIS
Event ID	5133
Event name	tmnxOesSwUpgdFailed
SNMP notification prefix and OID	TIMETRA-OES-MIB.tmnxOesNotifications.9
Default severity	minor
Message format string	OES software upgrade failed: *$tmnxOesEventReason$*
Cause	The tmnxOesSwUpgdFailed notification is generated when a failure occurs in upgrading a component in the OES. This notification is applicable at the NE (Network Element) level and/or the card level.
Effect	The component is not upgraded.
Recovery	1) Determine the reason the upgrade failed by checking the tmnx OesEventReason. First clear the condition indicated by the reason in the object tmnxOesEventReason. 2) Perform a soft reset on the card that failed to upgrade and try the upgrade procedure again. 3) Perform a hard reset on the card that failed to upgrade and try the upgrade procedure again. 4) Remove and re-insert the card that failed to upgrade and try the upgrade procedure again. 5) Replace the card that failed to upgrade and try the upgrade procedure again. 6) Inform the Nokia technical support team.

9.179 tmnxOesTempLow

Table 315: tmnxOesTempLow properties

Property name	Value
Application name	CHASSIS
Event ID	5128
Event name	tmnxOesTempLow
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.28
Default severity	major
Message format string	Class *$tmnxHwClass$*: Operational temperature too low
Cause	The tmnxOesTempLow notification is generated when the card has detected its temperature is below operational limits.
Effect	The card performance may degrade or may not work as expected.
Recovery	Ensure that no environmental issues exist where the network element resides. Resolve any existing issues.

9.180 tmnxOesTempLowClear

Table 316: tmnxOesTempLowClear properties

Property name	Value
Application name	CHASSIS
Event ID	5129
Event name	tmnxOesTempLowClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.29
Default severity	cleared
Message format string	Class *$tmnxHwClass$*: Operational temperature too low cleared
Cause	The tmnxOesFanSpeedLowClear notification is generated when the card has indicated its temperature is within operational limits.
Effect	The card resumes normal operation state.
Recovery	No recovery is required.

9.181 tmnxOesUsrpnlPortDown

Table 317: tmnxOesUsrpnlPortDown properties

Property name	Value
Application name	CHASSIS
Event ID	5103
Event name	tmnxOesUsrpnlPortDown
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.3
Default severity	minor
Message format string	OES USRPNL Port is not operational
Cause	The tmnxOesUsrpnlPortDown notification is generated when a port (E1 or E2) on an OES USRPNL card is not operational. The reason may be a misconnected, disconnected or faulty cable, or a faulty port or USRPNL.
Effect	If an E1 or E2 port is down then one of the control plane communication paths between the router and the OES Master Chassis is not available. The control communications with the OES may be affected rendering the OES chassis unmanageable. Other control communications paths may be available.
Recovery	Check that the cable is correctly connected and test the cable.

9.182 tmnxOesUsrpnlPortUp

Table 318: tmnxOesUsrpnlPortUp properties

Property name	Value
Application name	CHASSIS
Event ID	5104
Event name	tmnxOesUsrpnlPortUp
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.4
Default severity	minor
Message format string	OES USRPNL Port is operational

Property name	Value
Cause	The tmnxOesUsrpnlPortUp notification is generated when the OES USRPNL port is now operational.
Effect	If an E1 or E2 port is up then a control plane communication path between the router and the OES Master Chassis has been established and the OES can be managed by the router.
Recovery	No recovery required.

9.183 tmnxPeBootloaderVersionMismatch

Table 319: tmnxPeBootloaderVersionMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2027
Event name	tmnxPeBootloaderVersionMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.35
Default severity	major
Message format string	Class *$tmnxHwClass$* : Bootloader version mismatch - expected software version *$tmnxHwSoftwareCodeVersion$*, equipped version *$tmnxChassisNotifyMismatchedVer$*
Cause	Generated when there is a mismatch between the CPM and boot loader versions. tmnxChassisNotifyHwIndex identifies the CPM card. tmnxChassisNotifyMismatchedVer contains the mismatched version of bootloader and tmnxHwSoftwareCodeVersion contains the expected version of the bootloader.
Effect	N/A
Recovery	N/A

9.184 tmnxPeBootromVersionMismatch

Table 320: tmnxPeBootromVersionMismatch properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2028
Event name	tmnxPeBootromVersionMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.36
Default severity	major
Message format string	Class *$tmnxHwClass$* : Bootrom version mismatch - expected version *$tmnxHwSoftwareCodeVersion$*, equipped version *$tmnxChassis NotifyMismatchedVer$*
Cause	Generated when there is a mismatch between the boot rom versions. tmnxChassisNotifyHwIndex identifies the IOM card. tmnxChassisNotify MismatchedVer contains the mismatched version of bootrom and tmnx HwSoftwareCodeVersion contains the expected version of the bootrom.
Effect	N/A
Recovery	N/A

9.185 tmnxPeFirmwareVersionWarning

Table 321: tmnxPeFirmwareVersionWarning properties

Property name	Value
Application name	CHASSIS
Event ID	2082
Event name	tmnxPeFirmwareVersionWarning
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.70
Default severity	major
Message format string	Class *$tmnxHwClass$* : Firmware version *$tmnxHwFirmwareCode Version$* is compatible but not the latest. Hard reset the MDA/IMM to upgrade to the most recent firmware if desired.
Cause	Generated when a card is running compatible yet older firmware than the firmware associated with the current software release. tmnxChassis NotifyHwIndex identifies the card. The tmnxHwFirmwareCodeVersion object will contain the programmed the firmware version.
Effect	N/A
Recovery	N/A

9.186 tmnxPeFPGAVersionMismatch

Table 322: tmnxPeFPGAVersionMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2029
Event name	tmnxPeFPGAVersionMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.37
Default severity	major
Message format string	Class *$tmnxHwClass$* : FPGA version mismatch - expected version *$tmnxHwSoftwareCodeVersion$*, equipped version *$tmnxChassis NotifyMismatchedVer$*
Cause	Generated when there is a mismatch between the FPGA versions. tmnxChassisNotifyHwIndex identifies the IOM card. tmnxChassisNotify MismatchedVer contains the mismatched version of FPGA and tmnx HwSoftwareCodeVersion contains the expected version of the FPGA.
Effect	N/A
Recovery	N/A

9.187 tmnxPeSoftwareLoadFailed

Table 323: tmnxPeSoftwareLoadFailed properties

Property name	Value
Application name	CHASSIS
Event ID	2026
Event name	tmnxPeSoftwareLoadFailed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.34
Default severity	major
Message format string	Class *$tmnxHwClass$* : Failed to load software from *$tmnxChassis NotifySoftwareLocation$*
Cause	Generated when the CPM fails to load the software from a specified location. tmnxChassisNotifyHwIndex identifies the card for which the

Property name	Value
	software load failed and tmnxChassisNotifySoftwareLocation contains the location from where the software load was attempted.
Effect	N/A
Recovery	N/A

9.188 tmnxPeSoftwareVersionMismatch

Table 324: tmnxPeSoftwareVersionMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2025
Event name	tmnxPeSoftwareVersionMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.16
Default severity	major
Message format string	Class *$tmnxHwClass$* : Software version mismatch - expected software version *$tmnxHwSoftwareCodeVersion$*, equipped version *$tmnxChassisNotifyMismatchedVer$*
Cause	Generated when there is a mismatch between software versions of the active CPM and standby CPM or the CPM and IOM. tmnxChassisNotify HwIndex identifies the mismatched CPM/IOM card and tmnxChassis NotifyMismatchedVer will contain the version of the mismatched card. The tmnxHwSoftwareCodeVersion object will contain the expected version.
Effect	N/A
Recovery	N/A

9.189 tmnxPlcyAcctStatsEventOvrflw

Table 325: tmnxPlcyAcctStatsEventOvrflw properties

Property name	Value
Application name	CHASSIS
Event ID	2120

Property name	Value
Event name	tmnxPlcyAcctStatsEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.107
Default severity	minor
Message format string	Policy Accounting FP log event overflow occurred on card *$tmnx ChassisNotifyCardSlotNum$* at *$tmnxPlcyAcctTimeEventOccured$*.
Cause	The tmnxPlcyAcctStatsEventOvrflw notification is generated when tmnxPlcyAcctStatsPoolExcResource and tmnxPlcyAcctStatsPoolLow Resource occur more than 200 times because of resource usage fluctuation. The IOM raises the final trap to indicate overflow and stops logging traps.
Effect	Some FP notifications configured on the card may not be received.
Recovery	Notifications will resume once the Overflow clear is set.

9.190 tmnxPlcyAcctStatsEventOvrflwClr

Table 326: tmnxPlcyAcctStatsEventOvrflwClr properties

Property name	Value
Application name	CHASSIS
Event ID	2119
Event name	tmnxPlcyAcctStatsEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.106
Default severity	minor
Message format string	*$tmnxPlcyAcctMissingNotifCount$* Policy Accounting FP log events were dropped in the last event throttling interval on card *$tmnxChassis NotifyCardSlotNum$* at *$tmnxPlcyAcctTimeEventOccured$*.
Cause	The tmnxPlcyAcctStatsEventOvrflwClr notification is generated when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

9.191 tmnxPlcyAcctStatsPoolExcResource

Table 327: tmnxPlcyAcctStatsPoolExcResource properties

Property name	Value
Application name	CHASSIS
Event ID	2117
Event name	tmnxPlcyAcctStatsPoolExcResource
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.104
Default severity	minor
Message format string	Stats Resource usage on card *$tmnxCardSlotNum$* and forwarding plane *$tmnxFPNum$* exceeds 95 percent of the stats pool limit. Total stats resource used is ' *$tmnxFPPlcyAcctStatsInUse$*' and the limit is '*$tmnxFPPlcyAcctStatsPool$*'
Cause	The tmnxPlcyAcctStatsPoolExcResource notification is generated when the number of in-use stats resource usage as specified by tmnxFPPlcyAcctStatsInUse exceeds 95 percent of the stats pool limit as specified by tmnxFPPlcyAcctStatsPool.
Effect	The affected device may not provide accurate and complete statistics.
Recovery	There is no recovery required for this notification.

9.192 tmnxPlcyAcctStatsPoolLowResource

Table 328: tmnxPlcyAcctStatsPoolLowResource properties

Property name	Value
Application name	CHASSIS
Event ID	2118
Event name	tmnxPlcyAcctStatsPoolLowResource
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.105
Default severity	minor
Message format string	Stats Resource usage on card *$tmnxCardSlotNum$* and forwarding plane *$tmnxFPNum$* is below 85 percent of the stats pool limit. Total stats resource used is ' *$tmnxFPPlcyAcctStatsInUse$*' and the limit is '*$tmnxFPPlcyAcctStatsPool$*'

Property name	Value
Cause	The tmnxPlcyAcctStatsPoolLowResource notification is generated when the number of in-use stats resource as specified by tmnxFPPlcy AcctStatsInUse is below 85 percent of the stats pool limit as specified by tmnxFPPlcyAcctStatsPool.
Effect	The configured stats pool limit is cleared when the number of in-use stats resources falls below 85 percent of the stats pool limit.
Recovery	There is no recovery required for this notification.

9.193 tmnxPowerSupplyWrongFanDir

Table 329: tmnxPowerSupplyWrongFanDir properties

Property name	Value
Application name	CHASSIS
Event ID	2132
Event name	tmnxPowerSupplyWrongFanDir
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.119
Default severity	major
Message format string	The *$tmnxChassisPowerSupplyFanDir$* fan direction for power supply *$tmnxHwIndex$* is not supported.
Cause	The tmnxPowerSupplyWrongFanDir notification is generated when the airflow direction of the power supply's fan is incorrect.
Effect	The power supply is not cooling properly and may overheat.
Recovery	Replace the power supply with one that has the proper fan direction.

9.194 tmnxPowerSupplyWrongFanDirClear

Table 330: tmnxPowerSupplyWrongFanDirClear properties

Property name	Value
Application name	CHASSIS
Event ID	2133
Event name	tmnxPowerSupplyWrongFanDirClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.120
Default severity	major
Message format string	The fan direction for power supply *$tmnxHwIndex$* has been corrected.
Cause	The tmnxPowerSupplyWrongFanDirClear notification is generated when the airflow direction of the power supply's fan is corrected.
Effect	The fan is cooling the power supply in the proper direction.
Recovery	No recovery required.

9.195 tmnxRedPrimaryCPMFail

Table 331: tmnxRedPrimaryCPMFail properties

Property name	Value
Application name	CHASSIS
Event ID	2012
Event name	tmnxRedPrimaryCPMFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.21
Default severity	critical
Message format string	Active CPM failed
Cause	Generated when the primary CPM fails.
Effect	N/A
Recovery	N/A

9.196 tmnxSasAlarminput1StateChanged

Table 332: tmnxSasAlarminput1StateChanged properties

Property name	Value
Application name	CHASSIS
Event ID	3001

Property name	Value
Event name	tmnxSasAlarminput1StateChanged
SNMP notification prefix and OID	TIMETRA-SAS-ALARM-INPUT-MIB.tmnxSasAlarmInputNotifications.1
Default severity	major
Message format string	Alarm Input " *$tmnxSasAlarmInputDescription$*" ("*$tmnxSasAlarmInputNotifyId$*") has changed status to " *$tmnxSasAlarmOutputSeverity$*" "*$tmnxSasAlarmInputNotifyMessage$*"
Cause	A tmnxSasAlarminput1StateChanged notification is sent when status of the alarm input on pin one(1) changes. When this notification is sent, the field tmnxSasAlarmInputNotifyMessage is populated with either the tmnxSasAlarmInputTriggerMessage when the alarm is raised, or the tmnxSasAlarmInputClearMessage when the alarm is cleared. The trigger or clear actions depend on the polarity of the input as defined in tmnxSasAlarmInputPolarity.
Effect	A desirable or undesirable event has occurred in the external equipment connected to the alarm input. Hence the characteristics of effect and the associated risks vary depending on the nature of the external equipment being monitored over the alarm input.
Recovery	Check the external equipment, connected to the alarm input pin one(1), that resulted in this alarm and rectify the problem.

9.197 tmnxSasAlarminput2StateChanged

Table 333: tmnxSasAlarminput2StateChanged properties

Property name	Value
Application name	CHASSIS
Event ID	3002
Event name	tmnxSasAlarminput2StateChanged
SNMP notification prefix and OID	TIMETRA-SAS-ALARM-INPUT-MIB.tmnxSasAlarmInputNotifications.2
Default severity	major
Message format string	Alarm Input " *$tmnxSasAlarmInputDescription$*" ("*$tmnxSasAlarmInputNotifyId$*") has changed status to " *$tmnxSasAlarmOutputSeverity$*" "*$tmnxSasAlarmInputNotifyMessage$*"
Cause	A tmnxSasAlarminput2StateChanged notification is sent when status of the alarm input on pin two(2) changes. When this notification is sent, the field tmnxSasAlarmInputNotifyMessage is populated with either

Property name	Value
	the tmnxSasAlarmInputTriggerMessage when the alarm is raised, or the tmnxSasAlarmInputClearMessage when the alarm is cleared. The trigger or clear actions depend on the polarity of the input as defined in tmnxSasAlarmInputPolarity.
Effect	A desirable or undesirable event has occurred in the external equipment connected to the alarm input. Hence the characteristics of effect and the associated risks vary depending on the nature of the external equipment being monitored over the alarm input.
Recovery	Check the external equipment, connected to the alarm input pin two(2), that resulted in this alarm and rectify the problem.

9.198 tmnxSasAlarminput3StateChanged

Table 334: tmnxSasAlarminput3StateChanged properties

Property name	Value
Application name	CHASSIS
Event ID	3003
Event name	tmnxSasAlarminput3StateChanged
SNMP notification prefix and OID	TIMETRA-SAS-ALARM-INPUT-MIB.tmnxSasAlarmInputNotifications.3
Default severity	major
Message format string	Alarm Input " *$tmnxSasAlarmInputDescription$*" ("*$tmnxSasAlarmInputNotifyId$*") has changed status to " *$tmnxSasAlarmOutputSeverity$*" "*$tmnxSasAlarmInputNotifyMessage$*"
Cause	A tmnxSasAlarminput3StateChanged notification is sent when status of the alarm input on pin three(3) changes. When this notification is sent, the field tmnxSasAlarmInputNotifyMessage is populated with either the tmnxSasAlarmInputTriggerMessage when the alarm is raised, or the tmnxSasAlarmInputClearMessage when the alarm is cleared. The trigger or clear actions depend on the polarity of the input as defined in tmnxSasAlarmInputPolarity.
Effect	A desirable or undesirable event has occurred in the external equipment connected to the alarm input. Hence the characteristics of effect and the associated risks vary depending on the nature of the external equipment being monitored over the alarm input.
Recovery	Check the external equipment, connected to the alarm input pin three(3), that resulted in this alarm and rectify the problem.

9.199 tmnxSasAlarminput4StateChanged

Table 335: tmnxSasAlarminput4StateChanged properties

Property name	Value
Application name	CHASSIS
Event ID	3004
Event name	tmnxSasAlarminput4StateChanged
SNMP notification prefix and OID	TIMETRA-SAS-ALARM-INPUT-MIB.tmnxSasAlarmInputNotifications.4
Default severity	major
Message format string	Alarm Input " *$tmnxSasAlarmInputDescription$*" ("*$tmnxSasAlarmInputNotifyId$*") has changed status to " *$tmnxSasAlarmOutputSeverity$*" "*$tmnxSasAlarmInputNotifyMessage$*"
Cause	A tmnxSasAlarminput4StateChanged notification is sent when status of the alarm input on pin four(4) changes. When this notification is sent, the field tmnxSasAlarmInputNotifyMessage is populated with either the tmnxSasAlarmInputTriggerMessage when the alarm is raised, or the tmnxSasAlarmInputClearMessage when the alarm is cleared. The trigger or clear actions depend on the polarity of the input as defined in tmnxSasAlarmInputPolarity.
Effect	A desirable or undesirable event has occurred in the external equipment connected to the alarm input. Hence the characteristics of effect and the associated risks vary depending on the nature of the external equipment being monitored over the alarm input.
Recovery	Check the external equipment, connected to the alarm input pin four(4), that resulted in this alarm and rectify the problem.

9.200 tmnxSfmIcPortDDMClear

Table 336: tmnxSfmIcPortDDMClear properties

Property name	Value
Application name	CHASSIS
Event ID	4026
Event name	tmnxSfmIcPortDDMClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.7
Default severity	minor
Message format string	SFM interconnect port SFF DDM *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailedObject$*) cleared
Cause	The tmnxSfmIcPortDDMFailure notification is generated when an SFF in an SFM interconnect port that supports Digital Diagnostic Monitoring (DDM) clears a failed state.
Effect	N/A
Recovery	N/A

9.201 tmnxSfmIcPortDDMFailure

Table 337: tmnxSfmIcPortDDMFailure properties

Property name	Value
Application name	CHASSIS
Event ID	4025
Event name	tmnxSfmIcPortDDMFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.6
Default severity	minor
Message format string	SFM interconnect port SFF DDM *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailedObject$*) raised
Cause	The tmnxSfmIcPortDDMFailure notification is generated when an SFF in an SFM interconnect port that supports Digital Diagnostic Monitoring (DDM) enters a failed state.
Effect	N/A
Recovery	N/A

9.202 tmnxSfmIcPortDegraded

Table 338: tmnxSfmIcPortDegraded properties

Property name	Value
Application name	CHASSIS
Event ID	4027
Event name	tmnxSfmIcPortDegraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.8
Default severity	minor
Message format string	Switch fabric capacity associated with the SFM interconnect port is in a *$tmnxSfmIcPortDegradeState$* state
Cause	The tmnxSfmIcPortDegraded notification is generated when the system has detected a degradation of the switch fabric that is associated with a particular SFM interconnect port. The value of tmnxSfmIcPortDegrade State will reflect this condition by having a value that is NOT 'none (1)'. If the value of tmnxSfmIcPortDegradeState is 'degraded (2)' the SFM interconnect port can still carry some traffic but not at the full capacity of the port. The port and attached cable are not necessarily the cause of the degradation but are a likely cause.
Effect	Switch fabric capacity on this port is reduced when tmnxSfmIcPort DegradeState is degraded. This may not be causing any impact to service because of redundancy in the fabric.
Recovery	Although it may not be necessary to maintain full service, replacing the affected components may restore some fabric capacity."

9.203 tmnxSfmIcPortDegradedClear

Table 339: tmnxSfmIcPortDegradedClear properties

Property name	Value
Application name	CHASSIS
Event ID	4028
Event name	tmnxSfmIcPortDegradedClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.9

Property name	Value
Default severity	minor
Message format string	Switch fabric capacity associated with the SFM interconnect port is not in a degraded state
Cause	The tmnxSfmIcPortDegradedClear notification is generated when the switch fabric associated with the SFM interconnect port is not degraded. This occurs when the value of tmnxSfmIcPortDegradeState is 'none (1)'."
Effect	N/A
Recovery	N/A

9.204 tmnxSfmIcPortDown

Table 340: tmnxSfmIcPortDown properties

Property name	Value
Application name	CHASSIS
Event ID	4017
Event name	tmnxSfmIcPortDown
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.1
Default severity	minor
Message format string	Possible messages: • SFM interconnect port is not operational. Error code = *$tmnxSfmIcPortOperState$* to Fabric *$tmnxSfmIcPortMisconSfm$* IcPort *$tmnxSfmIcPortMisconSfmIcPort$* • SFM interconnect port is not operational. Error code = *$tmnxSfmIcPortOperState$*
Cause	The tmnxSfmIcPortDown alarm is generated when the SFM interconnect port is not operational. The reason may be a cable connected incorrectly, a disconnected cable, a faulty cable, or a misbehaving SFM interconnect port or SFM card.
Effect	This port can no longer be used as part of the user plane fabric between chassis. Other fabric paths may be available resulting in no loss of capacity.

Property name	Value
Recovery	A manual verification and testing of each SFM interconnect port is required to ensure fully functional operation. Physical replacement of cabling may be required.

9.205 tmnxSfmIcPortSFFInserted

Table 341: tmnxSfmIcPortSFFInserted properties

Property name	Value
Application name	CHASSIS
Event ID	4019
Event name	tmnxSfmIcPortSFFInserted
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.3
Default severity	minor
Message format string	SFM interconnect port SFF inserted
Cause	The tmnxSfmIcPortSFFInserted notification is generated when the Small Form Factor (SFF) pluggable optical module (eg. CXP) is inserted into an SFM interconnect port.
Effect	This event is for notification only.
Recovery	N/A

9.206 tmnxSfmIcPortSFFRemoved

Table 342: tmnxSfmIcPortSFFRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	4020
Event name	tmnxSfmIcPortSFFRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.4
Default severity	minor

Property name	Value
Message format string	SFM interconnect port SFF removed
Cause	The tmnxSfmIcPortSFFRemoved notification is generated when the SFF (eg. CXP) is removed from the SFM interconnect port.
Effect	Removing the module will cause the port to go down. This port can no longer be used as part of the user plane fabric between chassis. Other fabric paths may be available resulting in no loss of capacity.
Recovery	Insert a working SFF into the SFM interconnect port.

9.207 tmnxSfmIcPortUp

Table 343: tmnxSfmIcPortUp properties

Property name	Value
Application name	CHASSIS
Event ID	4018
Event name	tmnxSfmIcPortUp
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.2
Default severity	minor
Message format string	SFM interconnect port is operational
Cause	The tmnxSfmIcPortUp notification is generated when the SFM interconnect port is operational again.
Effect	This port can now be used as part of the user plane fabric between chassis.
Recovery	N/A

9.208 tmnxSyncIfTimBITS2048khzUnsup

Table 344: tmnxSyncIfTimBITS2048khzUnsup properties

Property name	Value
Application name	CHASSIS
Event ID	2134

Property name	Value
Event name	tmnxSyncIfTimBITS2048khzUnsup
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.123
Default severity	major
Message format string	The revision of *$tmnxHwIndex$* does not meet the specifications to support the 2048kHz BITS interface type.
Cause	The tmnxSyncIfTimBITS2048khzUnsup notification is generated when the value of tSyncIfTimingAdmBITSIfType is set to 'g703-2048khz (5)' and the CPM does not meet the specifications for the 2048kHz BITS output signal under G.703.
Effect	The BITS input will not be used as the Sync reference and the 2048k Hz BITS output signal generated by the CPM is squelched.
Recovery	Replace the CPM with one that is capable of generating the 2048k Hz BITS output signal, or set tSyncIfTimingAdmBITSIfType to a value other than 'g703-2048khz (5)'.

9.209 tmnxSyncIfTimBITS2048khzUnsupClr

Table 345: tmnxSyncIfTimBITS2048khzUnsupClr properties

Property name	Value
Application name	CHASSIS
Event ID	2135
Event name	tmnxSyncIfTimBITS2048khzUnsupClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.124
Default severity	major
Message format string	*$tmnxHwIndex$* has been replaced with a CPM that meets the specification for 2048kHz or the BITS interface type is no longer 2048k Hz.
Cause	The tmnxSyncIfTimBITS2048khzUnsupClr notification is generated when a tmnxSyncIfTimBITS2048khzUnsup notification is outstanding and the CPM was replaced with one that meets the specifications for the 2048kHz BITS output signal under G.703 or tSyncIfTiming AdmBITSIfType is set to a value other than 'g703-2048khz (5)'.
Effect	The CPM can now support the configuration of tSyncIfTiming AdmBITSIfType.

Property name	Value
Recovery	No recovery required.

10 DEBUG

10.1 traceEvent

Table 346: traceEvent properties

Property name	Value
Application name	DEBUG
Event ID	2001
Event name	traceEvent
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	*$subject$*: *$title$* *$message$*
Cause	The system generated a debug message.
Effect	Unknown.
Recovery	Contact Nokia customer service.

11 DHCP

11.1 sapDHCPLeaseEntriesExceeded

Table 347: sapDHCPLeaseEntriesExceeded properties

Property name	Value
Application name	DHCP
Event ID	2002
Event name	sapDHCPLeaseEntriesExceeded
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.9
Default severity	warning
Message format string	Lease state for (CiAddr = *$svcDhcpLseStateNewCiAddr$*, ChAddr = *$svcDhcpLseStateNewChAddr$*, leaseTime = *$svcDhcpClientLease$*) was not stored because the number of DHCP lease states on SAP *$sapEncapValue$* in service *$svcId$* has reached its upper limit
Cause	The sapDHCPLeaseEntriesExceeded notification is generated when the number of DHCP lease state entries on a given SAP reaches a user configurable upper limit. This limit is given by sapTlsDhcp LeasePopulate for a TLS service and by TIMETRA-VRTR-MIB::vRtr IfDHCPLeasePopulate for an IES or VPRN service.
Effect	N/A
Recovery	Investigate the cause of the excessive DHCP lease states.

11.2 sapDHCPLseStateMobilityError

Table 348: sapDHCPLseStateMobilityError properties

Property name	Value
Application name	DHCP
Event ID	2027
Event name	sapDHCPLseStateMobilityError
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.22

Property name	Value
Default severity	warning
Message format string	Unable to perform mobility check on SAP *$sapEncapValue$* in service *$svcId$*
Cause	The sapDHCPLseStateMobilityError notification indicates that the system was unable to perform a mobility check for this lease state.
Effect	N/A
Recovery	Contact Nokia customer service.

11.3 sapDHCPLseStateOverride

Table 349: sapDHCPLseStateOverride properties

Property name	Value
Application name	DHCP
Event ID	2003
Event name	sapDHCPLseStateOverride
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.10
Default severity	warning
Message format string	Existing lease state (ipAddr = *$svcDhcpLseStateOldCiAddr$*, macAddr = *$svcDhcpLseStateOldChAddr$*) on SAP *$sapEncapValue$* in service *$svcId$* overridden to (ipAddr = *$svcDhcpLseStateNewCiAddr$*, mac Addr = *$svcDhcpLseStateNewChAddr$*)
Cause	The sapDHCPLseStateOverride notification is generated when an existing DHCP lease state is overridden by a new lease state which has the same IP address but a different MAC address.
Effect	Informational.
Recovery	N/A

11.4 sapDHCPLseStatePopulateErr

Table 350: sapDHCPLseStatePopulateErr properties

Property name	Value
Application name	DHCP
Event ID	2005
Event name	sapDHCPLseStatePopulateErr
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.12
Default severity	warning
Message format string	Lease state table population error on SAP *$sapEncapValue$* in service *$svcId$ - $svcDhcpLseStatePopulateError$*
Cause	The sapDHCPLseStatePopulateErr notification indicates that the system was unable to update the DHCP Lease State table with the information contained in the DHCP ACK message.
Effect	The DHCP ACK message has been discarded.
Recovery	Contact Nokia customer service.

11.5 sapDHCPProxyServerError

Table 351: sapDHCPProxyServerError properties

Property name	Value
Application name	DHCP
Event ID	2013
Event name	sapDHCPProxyServerError
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.18
Default severity	warning
Message format string	DHCP Proxy error on SAP *$sapEncapValue$* in service *$svcId$ - $svc DhcpProxyError$*
Cause	The sapDHCPProxyServerError notification indicates that the system was unable to proxy DHCP requests.
Effect	N/A
Recovery	Contact Nokia customer service.

11.6 sapDHCPSuspiciousPcktRcvd

Table 352: sapDHCPSuspiciousPcktRcvd properties

Property name	Value
Application name	DHCP
Event ID	2004
Event name	sapDHCPSuspiciousPcktRcvd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.11
Default severity	warning
Message format string	Suspicious DHCP packet received on SAP *$sapEncapValue$* in service *$svcId$* - *$svcDhcpPacketProblem$*
Cause	The sapDHCPSuspiciousPcktRcvd notification is generated when a DHCP packet is received with suspicious content.
Effect	N/A
Recovery	Contact Nokia customer service.

11.7 sapStatHost6DynMacConflict

Table 353: sapStatHost6DynMacConflict properties

Property name	Value
Application name	DHCP
Event ID	2030
Event name	sapStatHost6DynMacConflict
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.58
Default severity	warning
Message format string	The system could not update the MAC address for static host *$sapStatHost6IpAddress$* on SAP:*$sapEncapValue$*, service:*$svcId$* - *$sapNotifyReason$*
Cause	The system failed to update the MAC address of a static IPv6 host.
Effect	The static IPv6 host has a MAC address that is not up to date.

Property name	Value
Recovery	The recovery action depends on the exact reason why the MAC update failed. This is clarified in the sapNotifyReason object.

11.8 sapStaticHostDynMacConflict

Table 354: sapStaticHostDynMacConflict properties

Property name	Value
Application name	DHCP
Event ID	2012
Event name	sapStaticHostDynMacConflict
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.16
Default severity	warning
Message format string	Trying to learn conflicting dynamic MAC address for static host *$staticHostDynamicMacIpAddress$* on SAP *$sapEncapValue$* (service *$svcId$*) - *$staticHostDynamicMacConflict$*
Cause	The sapStaticHostDynMacConflict notification indicates that the system is trying to learn a conflicting IP-only static host dynamic MAC address (sapStaticHostDynMacAddress).
Effect	N/A
Recovery	Contact Nokia customer service.

11.9 sdpBindDHCPLeaseEntriesExceeded

Table 355: sdpBindDHCPLeaseEntriesExceeded properties

Property name	Value
Application name	DHCP
Event ID	2006
Event name	sdpBindDHCPLeaseEntriesExceeded
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.10
Default severity	warning

Property name	Value
Message format string	Lease state for (CiAddr = *$svcDhcpLseStateNewCiAddr$*, ChAddr = *$svcDhcpLseStateNewChAddr$*, leaseTime = *$svcDhcpClientLease$*) was not stored because the number of DHCP lease states on SDP Bind *$sdpBindId$* in service *$svcId$* has reached its upper limit
Cause	The sdpBindDHCPLeaseEntriesExceeded notification is generated when the number of DHCP lease state entries on a given IES or VRPN spoke-SDP reaches the user configurable upper limit given by TIMETRA-VRTR-MIB::vRtrIfDHCPLeasePopulate.
Effect	N/A
Recovery	Investigate the cause of the excessive DHCP lease states.

11.10 sdpBindDHCPLseStateMobilityErr

Table 356: sdpBindDHCPLseStateMobilityErr properties

Property name	Value
Application name	DHCP
Event ID	2028
Event name	sdpBindDHCPLseStateMobilityErr
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.21
Default severity	warning
Message format string	Unable to perform mobility check on SDP Bind *$sdpBindId$* in service *$svcId$*
Cause	The sdpBindDHCPLseStateMobilityErr notification indicates that the system was unable to perform a mobility check for this lease state.
Effect	N/A
Recovery	Contact Nokia customer service.

11.11 sdpBindDHCPLseStateOverride

Table 357: sdpBindDHCPLseStateOverride properties

Property name	Value
Application name	DHCP

Property name	Value
Event ID	2007
Event name	sdpBindDHCPLseStateOverride
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.11
Default severity	warning
Message format string	Existing lease state (ipAddr = *$svcDhcpLseStateOldCiAddr$*, macAddr = *$svcDhcpLseStateOldChAddr$*) on SDP Bind *$sdpBindId$* in service *$svcId$* overridden to (ipAddr = *$svcDhcpLseStateNewCiAddr$*, mac Addr = *$svcDhcpLseStateNewChAddr$*)
Cause	The sdpBindDHCPLseStateOverride notification is generated when an existing DHCP lease state is overridden by a new lease state which has the same IP address but a different MAC address. This notification is only applicable to IES and VPRN spoke-SDPs.
Effect	Informational.
Recovery	N/A

11.12 sdpBindDHCPLseStatePopulateErr

Table 358: sdpBindDHCPLseStatePopulateErr properties

Property name	Value
Application name	DHCP
Event ID	2009
Event name	sdpBindDHCPLseStatePopulateErr
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.13
Default severity	warning
Message format string	Lease state table population error on SDP Bind *$sdpBindId$* in service *$svcId$* - *$svcDhcpLseStatePopulateError$*
Cause	The sdpBindDHCPLseStatePopulateErr notification indicates that the system was unable to update the DHCP Lease State table with the information contained in the DHCP ACK message. This notification is only applicable to IES and VPRN spoke-SDPs.
Effect	The DHCP ACK message has been discarded.
Recovery	Contact Nokia customer service.

11.13 sdpBindDHCPProxyServerError

Table 359: sdpBindDHCPProxyServerError properties

Property name	Value
Application name	DHCP
Event ID	2016
Event name	sdpBindDHCPProxyServerError
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.17
Default severity	warning
Message format string	DHCP Proxy error on SDP Bind *$sdpBindId$* in service *$svcId$* - *$svcDhcpProxyError$*
Cause	The sdpBindDHCPProxyServerError notification indicates that the system was unable to proxy DHCP requests.
Effect	N/A
Recovery	Contact Nokia customer service.

11.14 sdpBindDHCPSuspiciousPcktRcvd

Table 360: sdpBindDHCPSuspiciousPcktRcvd properties

Property name	Value
Application name	DHCP
Event ID	2008
Event name	sdpBindDHCPSuspiciousPcktRcvd
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.12
Default severity	warning
Message format string	Suspicious DHCP packet received on SDP Bind *$sdpBindId$* in service *$svcId$* - *$svcDhcpPacketProblem$*
Cause	The sdpBindDHCPSuspiciousPcktRcvd notification is generated when a DHCP packet is received with suspicious content.
Effect	N/A

Property name	Value
Recovery	Contact Nokia customer service.

11.15 svcDHCPLseStateRestoreProblem

Table 361: svcDHCPLseStateRestoreProblem properties

Property name	Value
Application name	DHCP
Event ID	2001
Event name	svcDHCPLseStateRestoreProblem
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.14
Default severity	warning
Message format string	Problem occured while processing DHCP lease state persistency record (CiAddr = *$svcDhcpRestoreLseStateCiAddr$*) - *$svcDhcp RestoreLseStateProblem$*
Cause	The svcDHCPLseStateRestoreProblem notification is generated when an error is detected while processing a persistency record.
Effect	N/A
Recovery	Contact Nokia customer service.

11.16 svcDHCPMiscellaneousProblem

Table 362: svcDHCPMiscellaneousProblem properties

Property name	Value
Application name	DHCP
Event ID	2029
Event name	svcDHCPMiscellaneousProblem
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.23
Default severity	warning
Message format string	*$tmnxFailureDescription$*

Property name	Value
Cause	The svcDHCPMiscellaneousProblem notification is generated on miscellaneous DHCP problems.
Effect	N/A
Recovery	Contact Nokia customer service.

11.17 tmnxVRtrDHCP6AssignedIllegSubnet

Table 363: tmnxVRtrDHCP6AssignedIllegSubnet properties

Property name	Value
Application name	DHCP
Event ID	2025
Event name	tmnxVRtrDHCP6AssignedIllegSubnet
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.26
Default severity	warning
Message format string	Dropped incoming message because the IP address (inetAddr = *$vRtrDHCP6AssignedNetAddr$*/*$vRtrDHCP6AssignedPrefixLen$*) assigned to client (inetAddr = *$vRtrDHCP6ClientNetAddr$*) does not match the subnet of the incoming interface *$vRtrIfName$*, or conflicts with an existing node IP address in service *$vRtrServiceId$* (vRtr *$vRtrID$*)
Cause	The tmnxVRtrDHCP6AssignedIllegSubnet notification is generated when an IP address assigned to the client does not match the subnet of the interface.
Effect	N/A
Recovery	Contact Nokia customer service.

11.18 tmnxVRtrDHCP6ClientMacUnresolved

Table 364: tmnxVRtrDHCP6ClientMacUnresolved properties

Property name	Value
Application name	DHCP
Event ID	2026

Property name	Value
Event name	tmnxVRtrDHCP6ClientMacUnresolved
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.27
Default severity	warning
Message format string	Received a relay reply for a client with an unresolved MAC address (inetAddr = *$vRtrDHCP6ClientNetAddr$*) on interface *$vRtrIfName$* in service *$vRtrServiceId$* (vRtr *$vRtrID$*)
Cause	The tmnxVRtrDHCP6ClientMacUnresolved notification is generated when a relay reply is received for a client, and the client's MAC address has not been resolved yet.
Effect	N/A
Recovery	Contact Nokia customer service.

11.19 tmnxVRtrDHCP6IllegalClientAddr

Table 365: tmnxVRtrDHCP6IllegalClientAddr properties

Property name	Value
Application name	DHCP
Event ID	2024
Event name	tmnxVRtrDHCP6IllegalClientAddr
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.25
Default severity	warning
Message format string	Dropped incoming message because the client source IP (inetAddr = *$vRtrDHCP6ClientNetAddr$*) does not match the subnet of the incoming interface *$vRtrIfName$*, or conflicts with an existing node IP address in service *$vRtrServiceId$* (vRtr *$vRtrID$*)
Cause	The tmnxVRtrDHCP6IllegalClientAddr notification is generated when an incoming message is dropped because the client's source IP does not match the subnet of the incoming interface.
Effect	N/A
Recovery	Contact Nokia customer service.

11.20 tmnxVRtrDHCP6LseStateOverride

Table 366: tmnxVRtrDHCP6LseStateOverride properties

Property name	Value
Application name	DHCP
Event ID	2022
Event name	tmnxVRtrDHCP6LseStateOverride
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.23
Default severity	warning
Message format string	Override existing lease state (inetAddr = *$vRtrDHCP6OldAssignedNetAddr$*/*$vRtrDHCP6OldAssignedPrefixLen$*, chAddr = *$vRtrDhcpLseStateOldChAddr$*, DUID = *$vRtrDHCP6OldClientId$*) on interface *$vRtrIfName$* in service *$vRtrServiceId$* (vRtr *$vRtrID$*) to (inetAddr = *$vRtrDHCP6AssignedNetAddr$*/*$vRtrDHCP6AssignedPrefixLen$*, chAddr = *$vRtrDhcpLseStateNewChAddr$*, DUID = *$vRtrDHCP6NewClientId$*) - *$vRtrDHCP6LeaseOverrideResult$*
Cause	The tmnxVRtrDHCP6LseStateOverride notification is generated when an existing DHCP6 lease state is overridden by a new lease state which has the same IP address but a different client ID.
Effect	Informational.
Recovery	N/A

11.21 tmnxVRtrDHCP6RelayLseStExceeded

Table 367: tmnxVRtrDHCP6RelayLseStExceeded properties

Property name	Value
Application name	DHCP
Event ID	2020
Event name	tmnxVRtrDHCP6RelayLseStExceeded
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.21
Default severity	warning
Message format string	Lease state for (inetAddr = *$vRtrDHCP6AssignedNetAddr$*/*$vRtrDHCP6AssignedPrefixLen$*, DUID = *$vRtrDHCP6NewClientId$*, leaseTime = *$svcDhcpClientLease$*) was not stored because the number of DHCP6 relay lease states on interface *$vRtrIfName$* in

Property name	Value
	service *$vRtrServiceId$* (vRtr *$vRtrID$*) has reached its upper limit of *$vRtrIfDHCP6LeasePopulate$*
Cause	The tmnxVRtrDHCP6RelayLseStExceeded notification is generated when the number of lease states populated by DHCP6 relay on an interface exceeds vRtrIfDHCP6LeasePopulate.
Effect	N/A
Recovery	Investigate the cause of the excessive DHCP lease states.

11.22 tmnxVRtrDHCP6RelayReplyStripUni

Table 368: tmnxVRtrDHCP6RelayReplyStripUni properties

Property name	Value
Application name	DHCP
Event ID	2023
Event name	tmnxVRtrDHCP6RelayReplyStripUni
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.24
Default severity	warning
Message format string	DHCP6 relay stripped unicast option from message relayed from server (inetAddr = *$vRtrDHCP6ServerNetAddr$*) in relay reply message on interface *$vRtrIfName$* in service *$vRtrServiceId$* (vRtr *$vRtrID$*)
Cause	The tmnxVRtrDHCP6RelayReplyStripUni notification is generated when a unicast option is stripped from a message relayed from a server to a client in a relay reply message.
Effect	Informational.
Recovery	N/A

11.23 tmnxVRtrDHCP6ServerLseStExceeded

Table 369: tmnxVRtrDHCP6ServerLseStExceeded properties

Property name	Value
Application name	DHCP

Property name	Value
Event ID	2021
Event name	tmnxVRtrDHCP6ServerLseStExceeded
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.22
Default severity	warning
Message format string	Lease state for (inetAddr = *$vRtrDHCP6AssignedNetAddr$*/*$vRtrDHCP6AssignedPrefixLen$*, DUID = *$vRtrDHCP6NewClientId$*, leaseTime = *$svcDhcpClientLease$*) was not stored because the number of DHCP6 server lease states on interface *$vRtrIfName$* in service *$vRtrServiceId$* (vRtr *$vRtrID$*) has reached its upper limit of *$vRtrIfDHCP6ServerMaxLeaseStates$*
Cause	The tmnxVRtrDHCP6ServerLseStExceeded notification is generated when the number of lease states populated by DHCP6 server on an interface exceeds vRtrIfDHCP6ServerMaxLeaseStates.
Effect	N/A
Recovery	Investigate the cause of the excessive DHCP lease states.

11.24 tmnxVRtrDHCPIfLseStatesExceeded

Table 370: tmnxVRtrDHCPIfLseStatesExceeded properties

Property name	Value
Application name	DHCP
Event ID	2014
Event name	tmnxVRtrDHCPIfLseStatesExceeded
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.20
Default severity	warning
Message format string	Lease state for (CiAddr = *$svcDhcpLseStateNewCiAddr$*, ChAddr = *$svcDhcpLseStateNewChAddr$*, leaseTime = *$svcDhcpClientLease$*) received on SAP *$sapEncapValue$* was not stored because the number of DHCP lease states on interface *$vRtrIfName$* in service *$vRtrServiceId$* (vRtr *$vRtrID$*) has reached its upper limit of *$vRtrIfDHCPLeasePopulate$*.
Cause	The tmnxVRtrDHCPIfLseStatesExceeded notification is generated when the number of lease states on an interface exceeds vRtrIfDHCPLeasePopulate.

Property name	Value
Effect	N/A
Recovery	Investigate the cause of the excessive DHCP lease states.

11.25 tmnxVRtrDHCPSuspiciousPcktRcvd

Table 371: tmnxVRtrDHCPSuspiciousPcktRcvd properties

Property name	Value
Application name	DHCP
Event ID	2010
Event name	tmnxVRtrDHCPSuspiciousPcktRcvd
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.14
Default severity	warning
Message format string	Suspicious DHCP packet received on interface *$vRtrIfIndex$* in service *$vRtrServiceId$ - $vRtrDhcpPacketProblem$*
Cause	The tmnxVRtrDHCPSuspiciousPcktRcvd notification is generated when a DHCP packet is received with suspicious content.
Effect	N/A
Recovery	Contact Nokia customer service.

12 DHCPS

12.1 tmnxDhcpsAddrAllocationFailure

Table 372: tmnxDhcpsAddrAllocationFailure properties

Property name	Value
Application name	DHCPS
Event ID	2035
Event name	tmnxDhcpsAddrAllocationFailure
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.35
Default severity	warning
Message format string	Server "*$tmnxDhcpSvrNotifServerName$*" could not allocate IP address to client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$*). Reason: *$tmnxDhcpSvrNotifString$*
Cause	The tmnxDhcpsAddrAllocationFailure notification is generated when a DHCP server instance could not allocate an address for a client. The reason could be that the DHCP server instance could not find a free address, or it could be a configuration issue.
Effect	The client does not get an IP address lease this time. The client will have to try again if it needs a lease from this system.
Recovery	The recovery action, if any, will depend on the reason.

12.2 tmnxDhcpsFoLeaseUpdateFailed

Table 373: tmnxDhcpsFoLeaseUpdateFailed properties

Property name	Value
Application name	DHCPS
Event ID	2008
Event name	tmnxDhcpsFoLeaseUpdateFailed
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.8

Property name	Value
Default severity	warning
Message format string	BNDUPD message could not be processed for DHCP lease (server Name= *$tmnxDhcpSvrNotifServerName$*, ipAddr=*$tmnxDhcpSvrNotifLeaseClientAddr$*) sender (mac= *$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID$*) -- reason: *$tmnxDhcpsFoLeaseFailureReason$*
Cause	The tmnxDhcpsFoLeaseUpdateFailed notification is generated when a Binding Database Update (BNDUPD) packet received from the failover peer, cannot be processed successfully. The failure reason can be one of the following: foShutdown : the failover state of this DHCP Server instance is 'shutdown'; expired : the lease received from the peer has expired; maxReached : the maximum number of leases is already reached; subnetNotFound : no valid subnet for this lease could be found; rangeNotFound : no valid include range for this lease could be found.
Effect	If this DHCP server instance would have to perform a failover switch, it may lease addresses that were already given in lease by the failover peer. The effect is the same regardless of the failure reason.
Recovery	The required recovery action depends on the failure reason: fo Shutdown : put the DHCP server instance in state 'inService'; put the DHCP server instance failover facility in state 'inService'; expired : ensure the system clocks of this system and its failover peer are synchronized; maxReached : no recovery is possible; subnetNot Found : configure a valid subnet for this lease; rangeNotFound : configure a valid include range for this lease.

12.3 tmnxDhcpsFoStateChange

Table 374: tmnxDhcpsFoStateChange properties

Property name	Value
Application name	DHCPS
Event ID	2007
Event name	tmnxDhcpsFoStateChange
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.7
Default severity	warning
Message format string	DHCP server *$tmnxDhcpServerCfgServerName$* changed failover state: *$tmnxDhcpsFoState$*.

Property name	Value
Cause	The failover state of the DHCP server instance changed.
Effect	The effect depends on the new failover state: init | failover is not operational; the DHCP server startUp | instance is not operational; shutdown : failover is not operational; the DHCP server instance is operational in standalone mode; noCommunication : the communication with the partner is lost; the DHCP server temporarily continues to operate as in normal failover state; partnerDown : the partner is assumed down; the DHCP server instance is leasing addresses from its remote ranges as well as its local ranges; normal : failover is operational; the DHCP server instance is leasing addresses from its local ranges.
Recovery	The required recovery action depends on the new failover state: init | no recovery is required; startUp | shutdown : put the DHCP server instance in state 'inService'; put the DHCP server instance failover facility in state 'inService'; noCommunication | repair the communication with the peer; partnerDown | normal : no recovery is required.

12.4 tmnxDhcpsLeaseOfferedExpired

Table 375: tmnxDhcpsLeaseOfferedExpired properties

Property name	Value
Application name	DHCPS
Event ID	2034
Event name	tmnxDhcpsLeaseOfferedExpired
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.34
Default severity	warning
Message format string	Lease offered by server " *$tmnxDhcpServerCfgServerName$*" ip-address "*$tmnxDhcpSvrLeaseClientAddress$*" to client (mac= *$tmnx DhcpSvrNotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID $* expired
Cause	The tmnxDhcpsLeaseOfferedExpired notification is generated when a DHCP lease that this system had offered to a client, expires while it is still in the 'offered' state, because this system did not receive a DHCP request message from the client.
Effect	The client does not get a lease this time. The client will have to try again if it needs a lease from this system.

Property name	Value
Recovery	The recovery action, if any, will depend on the reason of the expiry.

12.5 tmnxDhcpsPacketDropped

Table 376: tmnxDhcpsPacketDropped properties

Property name	Value
Application name	DHCPS
Event ID	2036
Event name	tmnxDhcpsPacketDropped
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.36
Default severity	warning
Message format string	Server "*$tmnxDhcpSvrNotifServerName$*" dropped a packet from client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID$*). Reason: *$tmnxDhcpSvrNotifString$*
Cause	The tmnxDhcpsPacketDropped notification is generated when a DHCP server instance dropped a DHCP packet it received.
Effect	Some client request fails. The client will have to try again.
Recovery	The recovery action, if any, will depend on the reason.

12.6 tmnxDhcpsPoolFoLeaseUpdateFailed

Table 377: tmnxDhcpsPoolFoLeaseUpdateFailed properties

Property name	Value
Application name	DHCPS
Event ID	2025
Event name	tmnxDhcpsPoolFoLeaseUpdateFailed
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.25
Default severity	warning
Message format string	BNDUPD message could not be processed for DHCP lease (server Name= *$tmnxDhcpServerCfgServerName$*, pool=*$tmnxDhcpServer*

Property name	Value
	PoolName$*s, ipAddr= *$tmnxDhcpSvrNotifLeaseClientAddr$*) sender (mac=*$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x *$tmnxDhcpSvr NotifClientDUID$*) -- reason: *$tmnxDhcpsFoLeaseFailureReason$
Cause	The tmnxDhcpsPoolFoLeaseUpdateFailed notification is generated when a Binding Database Update (BNDUPD) packet received from the failover peer, cannot be processed successfully. This notification is only generated for DHCP server instances with the value of tmnxDhcp ServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'.
Effect	N/A
Recovery	N/A

12.7 tmnxDhcpsPoolFoStateChange

Table 378: tmnxDhcpsPoolFoStateChange properties

Property name	Value
Application name	DHCPS
Event ID	2024
Event name	tmnxDhcpsPoolFoStateChange
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.22
Default severity	warning
Message format string	DHCP server *$tmnxDhcpServerCfgServerName$* pool *$tmnxDhcp ServerPoolName$* changed failover state: *$tmnxDhcpsPoolFoState$*.
Cause	The tmnxDhcpsPoolFoStateChange notification is generated when the failover state of the DHCP server instance pool changes. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'.
Effect	N/A
Recovery	N/A

12.8 tmnxDhcpSvrDeclineStaticAddr

Table 379: tmnxDhcpSvrDeclineStaticAddr properties

Property name	Value
Application name	DHCPS
Event ID	2005
Event name	tmnxDhcpSvrDeclineStaticAddr
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.5
Default severity	warning
Message format string	DHCP static IP address (serverName= *$tmnxDhcpSvrNotifServerName $*, ipAddr=*$tmnxDhcpSvrNotifLeaseClientAddr$*) is declined by client (HwAddr= *$tmnxDhcpSvrNotifMsgHwAddress$*)
Cause	The tmnxDhcpSvrDeclineStaticAddr notification is generated when a DHCP decline message is received from a DHCP client that has a static IP address assigned.
Effect	N/A
Recovery	Further investigation is required to determine the cause of the incorrect messages from the client.

12.9 tmnxDhcpSvrHostConflict

Table 380: tmnxDhcpSvrHostConflict properties

Property name	Value
Application name	DHCPS
Event ID	2002
Event name	tmnxDhcpSvrHostConflict
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.2
Default severity	warning
Message format string	DHCP server *$tmnxDhcpSvrNotifServerName$* detects IP address assignment conflict for host (name= *$tmnxDhcpSvrNotifHostName $*, type=*$tmnxDhcpSvrNotifHostType$*) sender (mac= *$tmnxDhcpSvr NotifMsgHwAddress$*); ipAddr=*$tmnxDhcpSvrNotifLeaseClientAddr$*. *$tmnxDhcpSvrNotifDescription$*

Property name	Value
Cause	The tmnxDhcpSvrHostConflict notification can be generated for hosts configured with a fixed IP address in the local user database. If such a host requests an IP address and the system detects that this IP address has already been handed out to another (dynamic) host, then the tmnxDhcpSvrHostConflict notification is generated. This notification is only generated for DHCP server instances with the value of tmnx DhcpServerCfgAddrType set to 'ipv4(1)'.
Effect	N/A
Recovery	Investigate the cause of the address conflict.

12.10 tmnxDhcpSvrIntLseConflict

Table 381: tmnxDhcpSvrIntLseConflict properties

Property name	Value
Application name	DHCPS
Event ID	2016
Event name	tmnxDhcpSvrIntLseConflict
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.16
Default severity	warning
Message format string	Internal lease conflict in server " *$tmnxDhcpSvrNotifServerName$*" client (mac=*$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x *$tmnxDhcpSvrNotifClientDUID$*)
Cause	The tmnxDhcpSvrIntLseConflict notification is generated for DHCP hosts trying to acquire an IP address that was handed through the local address assignment infrastructure, or the local address assignment infrastructure tries to use an IP address that was handed out to a DHCP client. This notification is only generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)'.
Effect	N/A
Recovery	N/A

12.11 tmnxDhcpSvrLeaseCreate

Table 382: tmnxDhcpSvrLeaseCreate properties

Property name	Value
Application name	DHCPS
Event ID	2018
Event name	tmnxDhcpSvrLeaseCreate
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.18
Default severity	warning
Message format string	Lease for server " *$tmnxDhcpServerCfgServerName$*" ip-address "*$tmnxDhcpSvrLeaseClientAddress$*" client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID$*) configuration created
Cause	The tmnxDhcpSvrLeaseCreate notification is generated when a DHCP host is created. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'.
Effect	N/A
Recovery	N/A

12.12 tmnxDhcpSvrLeaseDefaultTimers

Table 383: tmnxDhcpSvrLeaseDefaultTimers properties

Property name	Value
Application name	DHCPS
Event ID	2012
Event name	tmnxDhcpSvrLeaseDefaultTimers
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.12
Default severity	warning
Message format string	Reverted to default lease timers for DHCP lease (serverName= *$tmnxDhcpSvrNotifServerName$*, ipAddr=*$tmnxDhcpSvrNotifLeaseClientAddr$*) client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$* DUID= 0x*$tmnxDhcpSvrNotifClientDUID$*)-- *$tmnxDhcpSvrNotifDescription$*

Property name	Value
Cause	The tmnxDhcpSvrLeaseDefaultTimers notification is generated when, for a particular DHCP client, the system has reverted to default lease timer values, because the configuration of the lease timers was inconsistent. The lease renew time T1 and lease rebind time T2 have been reverted to the default values of 1/2 and 2/3 of the lease time. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'.
Effect	N/A
Recovery	N/A

12.13 tmnxDhcpSvrLeaseDelete

Table 384: tmnxDhcpSvrLeaseDelete properties

Property name	Value
Application name	DHCPS
Event ID	2019
Event name	tmnxDhcpSvrLeaseDelete
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.19
Default severity	warning
Message format string	Lease for server " *$tmnxDhcpServerCfgServerName$*" ip-address "*$tmnxDhcpSvrLeaseClientAddress$*" client (mac= *$tmnxDhcpSvr NotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID$* configuration deleted
Cause	The tmnxDhcpSvrLeaseDelete notification is generated when a DHCP host is deleted. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'.
Effect	N/A
Recovery	N/A

12.14 tmnxDhcpSvrLeaseModify

Table 385: tmnxDhcpSvrLeaseModify properties

Property name	Value
Application name	DHCPS
Event ID	2017
Event name	tmnxDhcpSvrLeaseModify
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.17
Default severity	warning
Message format string	Lease for server " *$tmnxDhcpServerCfgServerName$*" ip-address "*$tmnxDhcpSvrLeaseClientAddress$*" client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID$*) configuration modified
Cause	The tmnxDhcpSvrLeaseModify notification is generated when a DHCP host is modified. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'.
Effect	N/A
Recovery	N/A

12.15 tmnxDhcpSvrLeaseNotOwner

Table 386: tmnxDhcpSvrLeaseNotOwner properties

Property name	Value
Application name	DHCPS
Event ID	2004
Event name	tmnxDhcpSvrLeaseNotOwner
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.4
Default severity	warning
Message format string	DHCP lease (serverName= *$tmnxDhcpSvrNotifServerName$*, ipAddr= *$tmnxDhcpSvrNotifLeaseClientAddr$*, ipAddrLen= *$tmnxDhcpSvrNotifLeaseClientAddrLen$*) is not owned by sender of DHCP message (Hw Addr= *$tmnxDhcpSvrNotifMsgHwAddress$*, DUID=0x*$tmnxDhcpSvrNotifClientDUID$*) *$tmnxDhcpSvrNotifDescription$*

Property name	Value
Cause	The tmnxDhcpSvrLeaseNotOwner notification is generated when a DHCP message is received from a DHCP client that does not own the lease indicated by the IP address from the message.
Effect	N/A
Recovery	Further investigation is required to determine the cause of the incorrect messages from the client.

12.16 tmnxDhcpSvrMaxLeasesReached

Table 387: tmnxDhcpSvrMaxLeasesReached properties

Property name	Value
Application name	DHCPS
Event ID	2010
Event name	tmnxDhcpSvrMaxLeasesReached
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.10
Default severity	warning
Message format string	The maximum number of leases (*$tmnxDhcpSvrMaxLeases$*) has been reached -- dropping DHCP message from sender (mac= *$tmnx DhcpSvrNotifMsgHwAddress$* DUID=0x*$tmnxDhcpSvrNotifClientDUID $*)
Cause	The tmnxDhcpSvrMaxLeasesReached notification is generated when any local DHCP server instance drops a DHCP message because the maximum number of leases was reached.
Effect	No DHCP server instances can lease any addresses.
Recovery	No recovery is possible.

12.17 tmnxDhcpSvrMsgTooLong

Table 388: tmnxDhcpSvrMsgTooLong properties

Property name	Value
Application name	DHCPS
Event ID	2006

Property name	Value
Event name	tmnxDhcpSvrMsgTooLong
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.6
Default severity	warning
Message format string	DHCP server *$tmnxDhcpSvrNotifServerName$* outgoing message to client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$*, DUID=0x*$tmnxDhcpSvrNotifClientDUID$*) too long (max size= *$tmnxDhcpSvrNotifMsgSizeLimit$*)
Cause	The actual length of the DHCP message being built exceeds the maximum size. The maximum size is the minimum of either the maximum DHCP message size or the size provided by the client in the option 'maximum DHCP message size'. A reason can be that too many options are defined on host, pool and subnet levels.
Effect	The Local DHCP Server cannot reply to the client's DHCP requests. The client cannot get an IP address from this DHCP Server.
Recovery	Reduce the number of DHCP options defined on host, pool and subnet levels. Or, if possible, modify the client's DHCP configuration to increase the 'maximum DHCP message size'.

12.18 tmnxDhcpSvrNoContFreeBlocks

Table 389: tmnxDhcpSvrNoContFreeBlocks properties

Property name	Value
Application name	DHCPS
Event ID	2022
Event name	tmnxDhcpSvrNoContFreeBlocks
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.20
Default severity	warning
Message format string	Lease creation failed, no contiguous free blocks on server= *$tmnxDhcpServerCfgServerName$*, link-address=*$tmnxDhcpSvrNotifLinkAddr$*, pri-pool= *$tmnxDhcpSvrNotifPrimaryPool$*, sec-pool=*$tmnxDhcpSvrNotifSecondaryPool$*, client DUID=0x *$tmnxDhcpSvrNotifClientDUID$*. Reason: *$tmnxDhcpSvrNotifString$*
Cause	The tmnxDhcpSvrNoContFreeBlocks notification is generated when a lease cannot be created because not enough contiguous blocks are found for the requested delegated prefix size. This notification is

Property name	Value
	only generated for DHCP server instances with the value of tmnxDhcp ServerCfgAddrType set to 'ipv6(2)'. More detailed information about the failure is indicated in the tmnxDhcpSvrNotifString object.
Effect	N/A
Recovery	N/A

12.19 tmnxDhcpSvrNoSubnetFixAddr

Table 390: tmnxDhcpSvrNoSubnetFixAddr properties

Property name	Value
Application name	DHCPS
Event ID	2011
Event name	tmnxDhcpSvrNoSubnetFixAddr
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.11
Default severity	warning
Message format string	DHCP server *$tmnxDhcpSvrNotifServerName$* could not find subnet for fixed IP address *$tmnxDhcpSvrNotifLeaseClientAddr$* of host (db name =*$tmnxDhcpSvrNotifUserDatabaseName$*, host name= *$tmnx DhcpSvrNotifHostName$*, type=*$tmnxDhcpSvrNotifHostType$*) -- dropping DHCP message from sender (mac= *$tmnxDhcpSvrNotifMsg HwAddress$*)
Cause	The tmnxDhcpSvrNoSubnetFixAddr notification can be generated for hosts configured with a fixed IP address in the local user database. If such a host requests an IP address and the system cannot find a matching subnet in this server instance for this IP address, then the tmnxDhcpSvrNoSubnetFixAddr notification is generated, and the request is dropped. This notification is only generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)'.
Effect	The Local DHCP Server cannot reply to the client's DHCP requests. The client cannot get an IP address from this DHCP Server.
Recovery	Either configure another fixed IP address for this host, or configure a new subnet in this server instance.

12.20 tmnxDhcpSvrPfxThDepletedV6

Table 391: tmnxDhcpSvrPfxThDepletedV6 properties

Property name	Value
Application name	DHCPS
Event ID	2033
Event name	tmnxDhcpSvrPfxThDepletedV6
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.33
Default severity	warning
Message format string	No free prefixes with minimum threshold length *$tmnxDhcpsPfxMinFreePrefixLen$* in prefix '*$tmnxDhcpSvrSubnetAddress$*/ *$tmnxDhcpSvrSubnetPrefixLength$*' in server '*$tmnxDhcpServerCfgServerName$*'.
Cause	The tmnxDhcpSvrPfxThDepletedV6 notification is generated when the actual number of free prefixes with minimum free threshold length available in the considered prefix becomes zero.
Effect	No more prefixes with minimum free threshold length are available in considered prefix.
Recovery	The operator may create additional prefixes in the considered prefix. Alternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.

12.21 tmnxDhcpSvrPfxThTooLowV6

Table 392: tmnxDhcpSvrPfxThTooLowV6 properties

Property name	Value
Application name	DHCPS
Event ID	2032
Event name	tmnxDhcpSvrPfxThTooLowV6
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.32
Default severity	warning
Message format string	The number of prefixes with minimum threshold length in prefix '...' is becoming low. *$tmnxDhcpsPfxThCurrFreeBlksHw$*/*$tmnxDhcpsPfx*

Property name	Value
	ThCurrFreeBlksLw$* free prefix(es). (Minimum free threshold *$tmnx DhcpsPfxMinFreePercent$*%/*$tmnxDhcpsPfxMinFreeNumber$)
Cause	The tmnxDhcpSvrPfxThTooLowV6 notification is generated when the actual number of free prefixes with minimum free threshold length available in the considered prefix is becoming too low.
Effect	Only a limited number of free prefixes with minimum free threshold length are available in the considered prefix.
Recovery	The operator may create additional prefixes in the considered prefix to prevent a shortage of available prefixes with minimum free threshold length. Alternatively, examination of the leases in the prefix may reveal that the distribution is not appropriate.

12.22 tmnxDhcpSvrPlThDepletedV6

Table 393: tmnxDhcpSvrPlThDepletedV6 properties

Property name	Value
Application name	DHCPS
Event ID	2031
Event name	tmnxDhcpSvrPlThDepletedV6
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.31
Default severity	warning
Message format string	No free prefixes with minimum threshold length *$tmnxDhcpsPlMinFree PrefixLen$* in pool '*$tmnxDhcpServerPoolName$*' in server ' *$tmnx DhcpServerCfgServerName$*'.
Cause	The tmnxDhcpSvrPlThDepletedV6 notification is generated when the actual number of free prefixes with minimum free threshold length available in the pool becomes zero.
Effect	No more free prefixes with minimum free threshold length are available in the pool.
Recovery	The operator may create additional prefixes in the pool. Alternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.

12.23 tmnxDhcpSvrPlThTooLowV6

Table 394: tmnxDhcpSvrPlThTooLowV6 properties

Property name	Value
Application name	DHCPS
Event ID	2030
Event name	tmnxDhcpSvrPlThTooLowV6
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.30
Default severity	warning
Message format string	The number of prefixes with minimum threshold length in pool ' *$tmnxDhcpSvrPoolName$*' is becoming low. *$tmnxDhcpsPlThCurrFreeBlksHw$*/ *$tmnxDhcpsPlThCurrFreeBlksLw$* free prefix(es). (Minimum free threshold *$tmnxDhcpsPlMinFreePercent$*%)
Cause	The tmnxDhcpSvrPlThTooLowV6 notification is generated when the actual number of free prefixes with minimum free threshold length available in the pool is becoming too low.
Effect	Only a limited number of free prefixes with minimum free threshold length are available in the pool.
Recovery	The operator may create additional prefixes in the pool to prevent a shortage of available prefixes with minimum free threshold length. Alternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.

12.24 tmnxDhcpSvrPoolDepleted

Table 395: tmnxDhcpSvrPoolDepleted properties

Property name	Value
Application name	DHCPS
Event ID	2015
Event name	tmnxDhcpSvrPoolDepleted
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.15
Default severity	warning
Message format string	No free addresses in pool " *$tmnxDhcpServerPoolName$*"

Property name	Value
Cause	The tmnxDhcpSvrPoolDepleted notification is generated when the actual number of free addresses becomes zero. This notification is only generated for DHCP server instances with the value of tmnxDhcp ServerCfgAddrType set to 'ipv4(1)'.
Effect	N/A
Recovery	N/A

12.25 tmnxDhcpSvrPoolMinFreeExc

Table 396: tmnxDhcpSvrPoolMinFreeExc properties

Property name	Value
Application name	DHCPS
Event ID	2013
Event name	tmnxDhcpSvrPoolMinFreeExc
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.13
Default severity	warning
Message format string	The number of free addresses (*$tmnxDhcpSvrNotifPoolFree$*) has fallen below the desired minimum (*$tmnxDhcpServerPoolMinFree$*) in pool "*$tmnxDhcpServerPoolName$*"
Cause	The tmnxDhcpSvrPoolMinFreeExc notification is generated when the actual number of free addresses in a pool falls below the desired minimum number.
Effect	If the actual number of free addresses in the pool kept falling, and if it reached zero, no more addresses in this pool would be available for new DHCP hosts.
Recovery	The operator may create additional ranges in the subnet(s), or create an additional subnet. Alternatively, examination of the leases in the pool may reveal that the address distribution is not appropriate.

12.26 tmnxDhcpSvrPoolUnknown

Table 397: tmnxDhcpSvrPoolUnknown properties

Property name	Value
Application name	DHCPS
Event ID	2003
Event name	tmnxDhcpSvrPoolUnknown
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.3
Default severity	warning
Message format string	DHCP server *$tmnxDhcpSvrNotifServerName$* detects an unknown pool (*$tmnxDhcpSvrNotifUnknownPoolName$*). *$tmnxDhcpSvrNotif Description$* sender (mac= *$tmnxDhcpSvrNotifMsgHwAddress$*, DUID=0x*$tmnxDhcpSvrNotifClientDUID$*)
Cause	The tmnxDhcpServerPoolUnknown notification is generated when the lookup in the local user database for a host returns a pool name which is not defined within the local DHCP server.
Effect	The DHCP server may not be able to serve an IP address.
Recovery	Investigate the cause of the invalid pool name, likely a configuration error.

12.27 tmnxDhcpSvrSubnetDepleted

Table 398: tmnxDhcpSvrSubnetDepleted properties

Property name	Value
Application name	DHCPS
Event ID	2014
Event name	tmnxDhcpSvrSubnetDepleted
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.14
Default severity	warning
Message format string	No free addresses in subnet *$tmnxDhcpSvrSubnetAddress$*/*$tmnx DhcpSvrSubnetPrefixLength$*
Cause	The tmnxDhcpSvrSubnetDepleted notification is generated when the actual number of free addresses becomes zero. This notification is

Property name	Value
	only generated for DHCP server instances with the value of tmnxDhcp ServerCfgAddrType set to 'ipv4(1)'.
Effect	N/A
Recovery	N/A

12.28 tmnxDhcpSvrSubnetMinFreeExc

Table 399: tmnxDhcpSvrSubnetMinFreeExc properties

Property name	Value
Application name	DHCPS
Event ID	2001
Event name	tmnxDhcpSvrSubnetMinFreeExc
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.1
Default severity	warning
Message format string	The number of free addresses (*$tmnxDhcpSvrSubnetStatsFree$*) has fallen below the desired minimum (*$tmnxDhcpSvrSubnetMinFree$*) in subnet *$tmnxDhcpSvrSubnetAddress$*/ *$tmnxDhcpSvrSubnetPrefix Length$*
Cause	The tmnxDhcpSvrSubnetMinFreeExc notification is generated when the actual number of free addresses in a subnet falls below the desired minimum number.
Effect	If the actual number of free addresses in the subnet kept falling, and if it reached zero, no more addresses in this subnet would be available for new DHCP hosts.
Recovery	The operator may create additional ranges in the subnet, or create an additional subnet. Alternatively, examination of the leases in the subnet may reveal that the address distribution is not appropriate.

12.29 tmnxDhcpSvrUserDbUnknown

Table 400: tmnxDhcpSvrUserDbUnknown properties

Property name	Value
Application name	DHCPS

Property name	Value
Event ID	2009
Event name	tmnxDhcpSvrUserDbUnknown
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.9
Default severity	warning
Message format string	User database *$tmnxDhcpServerCfgUserDatabase$* specified for server *$tmnxDhcpServerCfgServerName$* does not exist -- dropping DHCP message from sender (mac= *$tmnxDhcpSvrNotifMsg HwAddress$*)
Cause	The tmnxDhcpSvrUserDbUnknown notification is generated when the local DHCP server instance drops a DHCP message because a local user database with the name specified for this server instance could not be found. This notification is only generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)'.
Effect	This DHCP server instance cannot lease any addresses.
Recovery	Either reset the object tmnxDhcpServerCfgUserDatabase to its default value, or specify the name of an existing user database.

12.30 tmnxLudbDhcpGroupIfTooLong

Table 401: tmnxLudbDhcpGroupIfTooLong properties

Property name	Value
Application name	DHCPS
Event ID	2020
Event name	tmnxLudbDhcpGroupIfTooLong
SNMP notification prefix and OID	TIMETRA-LOCAL-USER-DB-MIB.tmnxLocalUserDbNotifications.1
Default severity	warning
Message format string	"*$tmnxLocUsrDbDhcpDefMsapGroupIf$*" concatenated with " *$tmnx LudbNotifyPortId$*" is too long.
Cause	The tmnxLudbDhcpGroupIfTooLong notification is generated when the default MSAP group interface name concatenated with the port-id is longer than 32 characters.
Effect	N/A

Property name	Value
Recovery	N/A

12.31 tmnxLudbPppoeGroupIfTooLong

Table 402: tmnxLudbPppoeGroupIfTooLong properties

Property name	Value
Application name	DHCPS
Event ID	2021
Event name	tmnxLudbPppoeGroupIfTooLong
SNMP notification prefix and OID	TIMETRA-LOCAL-USER-DB-MIB.tmnxLocalUserDbNotifications.2
Default severity	warning
Message format string	"*$tmnxLocUsrDbPppoeDefMsapGroupIf$*" concatenated with " *$tmnxLudbNotifyPortId$*" is too long.
Cause	The tmnxLudbPppoeGroupIfTooLong notification is generated when the default MSAP group interface name concatenated with the port-id is longer than 32 characters.
Effect	N/A
Recovery	N/A

13 DIAMETER

13.1 tmnxDiamAppSessionFailure

Table 403: tmnxDiamAppSessionFailure properties

Property name	Value
Application name	DIAMETER
Event ID	2003
Event name	tmnxDiamAppSessionFailure
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.3
Default severity	minor
Message format string	DIAMETER session failure, sessid= *$tmnxDiamAppSessionId$*, subscrid=*$tmnxDiamAppSubscrId$*, sapid= *$tmnxDiamAppSapId$*, slaprof=*$tmnxDiamAppSLAProfName$*, *$tmnxDiamAppTrapDescription$*
Cause	The tmnxDiamAppSessionFailure notification indicates that the DIAMETER protocol has a session failure.
Effect	Determined by cc-failure-handling settings.
Recovery	N/A

13.2 tmnxDiamMessageDropped

Table 404: tmnxDiamMessageDropped properties

Property name	Value
Application name	DIAMETER
Event ID	2007
Event name	tmnxDiamMessageDropped
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.7
Default severity	minor

Property name	Value
Message format string	Diameter message dropped, policy= *$tmnxDiamPlcyName$*, peer= *$tmnxDiamPeerStatsPeerName$*, client-side-peer-ip= *$tmnxDiamPeerStatsPeerIpAddr$*, tcp-port=*$tmnxDiamPeerStatsPeerPort$*, drop-count= *$tmnxDiamPeerStatsFailedMessages$*, *$tmnxDiamAppTrapDescription$*
Cause	The tmnxDiamMessageDropped notification indicates that the DIAMETER protocol has dropped a message.
Effect	N/A
Recovery	N/A

13.3 tmnxDiamPolicyPeerStateChange

Table 405: tmnxDiamPolicyPeerStateChange properties

Property name	Value
Application name	DIAMETER
Event ID	2001
Event name	tmnxDiamPolicyPeerStateChange
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.1
Default severity	minor
Message format string	DIAMETER policy *$tmnxDiamPlcyName$*, peer *$tmnxDiamPlcyPeerName$* now has operational state: PrimarySecundary = *$tmnxDiamPeerPrimarySecondary$*, connectionSuspended = *$tmnxDiamPeerConnectionSuspended$* and cooldownSeqActive = *$tmnxDiamPeerCooldownSeqActive$*, *$tmnxDiamAppTrapDescription$*
Cause	The state of the diameter policy peer changed.
Effect	N/A
Recovery	No recovery is necessary.

13.4 tmnxDiamPpPrxMcLocStateChanged

Table 406: tmnxDiamPpPrxMcLocStateChanged properties

Property name	Value
Application name	DIAMETER
Event ID	2005
Event name	tmnxDiamPpPrxMcLocStateChanged
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.5
Default severity	minor
Message format string	The proxy multi-chassis redundancy state of the Diameter peer policy *$tmnxDiamPlcyName$* changed to *$tmnxDiamPpPrxMcLocState$*
Cause	The MCS (Multi Chassis redundancy Synchronization) state of a proxy function has changed.
Effect	The effect depends on the actual state transition. The states 'active' and 'standby' are normal states. In other states, Diameter communication may be interrupted, and hosts may be refused access to network services.
Recovery	The need for recovery action depends on the state transition. In the states 'active' and 'standby', no recovery action may be necessary.

13.5 tmnxDiamSessionEvent

Table 407: tmnxDiamSessionEvent properties

Property name	Value
Application name	DIAMETER
Event ID	2004
Event name	tmnxDiamSessionEvent
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.4
Default severity	minor
Message format string	Session event, session ID=' *$tmnxDiamAppSessionId$*', policy='*$tmnx DiamAppPlcyId$*', application= *$tmnxDiamAppPlcyApplication$*, event= *$tmnxDiamNotifyEventId$*, *$tmnxDiamAppTrapDescription$*
Cause	A Diameter session has experienced a problem. The session ID is indicated with the tmnxDiamAppSessionId. The associated Diameter

Property name	Value
	application policy is indicated with the tmnxDiamAppPlcyApplication. What happened is indicated with the tmnxDiamNotifyEventId and the tmnxDiamAppTrapDescription.
Effect	The effect depends on the cause. For example: if a Diameter message could not be transmitted, session set-up may fail.
Recovery	The recovery depends on the cause.

14 DYNSVC

14.1 tmnxDynSvcSapFailed

Table 408: tmnxDynSvcSapFailed properties

Property name	Value
Application name	DYNSVC
Event ID	2001
Event name	tmnxDynSvcSapFailed
SNMP notification prefix and OID	TIMETRA-DYNAMIC-SERVICES-MIB.tmnxDynSvcNotifications.1
Default severity	minor
Message format string	The requested action for control-session *$tmnxDynSvcNotifSap AcctSessionId$* (SAP *$tmnxDynSvcNotifSapPortId$*) could not be completed - *$tmnxDynSvcNotifDescription$*
Cause	The tmnxDynSvcSapFailed notification is sent when a Dynamic Services service SAP creation, modification or removal failed.
Effect	The desired new configuration is not in effect; the system has returned to the original configuration if possible.
Recovery	No recovery is necessary when the original configuration could be restored.

15 EFM_OAM

15.1 dot3OamNonThresholdEvent

Table 409: dot3OamNonThresholdEvent properties

Property name	Value
Application name	EFM_OAM
Event ID	2005
Event name	dot3OamNonThresholdEvent
SNMP notification prefix and OID	DOT3-OAM-MIB.dot3OamNotifications.2
Default severity	minor
Message format string	Port *$ifIndex$* raised *$dot3OamEventLogLocation$* fault *$dot3Oam EventLogType$*
Cause	A dot3OamNonThresholdEvent notification is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event. This notification should not be sent more than once per second. The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance of the dot3OamEventLogTable. The management entity should periodically check dot3OamEventLogTable to detect any missed events.
Effect	N/A
Recovery	N/A

15.2 dot3OamThresholdEvent

Table 410: dot3OamThresholdEvent properties

Property name	Value
Application name	EFM_OAM
Event ID	2004

Property name	Value
Event name	dot3OamThresholdEvent
SNMP notification prefix and OID	DOT3-OAM-MIB.dot3OamNotifications.1
Default severity	major
Message format string	Port *$ifIndex$* raised *$dot3OamEventLogLocation$* SF fault *$dot3OamEventLogType$* - *$dot3OamEventLogValue$* errors exceeded the *$dot3OamEventLogThresholdLo$* error threshold during the *$dot3OamEventLogWindowLo$* decisecond window
Cause	A dot3OamThresholdEvent notification is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event. This notification should not be sent more than once per second. The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance in the dot3OamEventLogTable. The management entity should periodically check dot3OamEventLogTable to detect any missed events.
Effect	N/A
Recovery	N/A

15.3 tmnxDot3OamLoopCleared

Table 411: tmnxDot3OamLoopCleared properties

Property name	Value
Application name	EFM_OAM
Event ID	2003
Event name	tmnxDot3OamLoopCleared
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.3
Default severity	minor
Message format string	Loop cleared on port *$subject$*
Cause	The tmnxDot3OamLoopCleared notification is generated if efm-oam is enabled and the protocol stops receiving PDUs with the source MAC address equal to the MAC address of the port it was received on.
Effect	N/A

Property name	Value
Recovery	N/A

15.4 tmnxDot3OamLoopDetected

Table 412: tmnxDot3OamLoopDetected properties

Property name	Value
Application name	EFM_OAM
Event ID	2002
Event name	tmnxDot3OamLoopDetected
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.2
Default severity	minor
Message format string	Loop detected on port *$subject$*
Cause	The tmnxDot3OamLoopDetected notification is generated if efm-oam is enabled and the protocol receives a PDU with the source MAC address equal to the MAC address of the port it was received on. Only the first such PDU will cause the notification to be generated.
Effect	N/A
Recovery	N/A

15.5 tmnxDot3OamNonThresholdEventClr

Table 413: tmnxDot3OamNonThresholdEventClr properties

Property name	Value
Application name	EFM_OAM
Event ID	2008
Event name	tmnxDot3OamNonThresholdEventClr
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.6
Default severity	minor
Message format string	Port *$ifIndex$* cleared *$dot3OamEventLogLocation$* fault *$dot3OamEventLogType$*

Property name	Value
Cause	The tmnxDot3OamNonThresholdEventClr notification is generated when the local or remote non-threshold crossing event (DOT3-OAM-MIB::dot3OamNonThresholdEvent) is cleared on the port.
Effect	This non-threshold crossing event is no longer a potential cause for the port to restrict user traffic.
Recovery	There is no recovery for this notification.

15.6 tmnxDot3OamPeerChanged

Table 414: tmnxDot3OamPeerChanged properties

Property name	Value
Application name	EFM_OAM
Event ID	2001
Event name	tmnxDot3OamPeerChanged
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.1
Default severity	minor
Message format string	Peer MAC for port *$subject$* has changed to *$dot3OamPeerMac Address$*
Cause	The tmnxDot3OamPeerChanged notification is generated when the peer information (specifically the Peer MAC address) changes. Note that this notification will only be sent out if the peer information was previously available and the information changed, and not when the peer information is first learned or becomes unavailable.
Effect	N/A
Recovery	N/A

15.7 tmnxDot3OamSdThresholdEvent

Table 415: tmnxDot3OamSdThresholdEvent properties

Property name	Value
Application name	EFM_OAM
Event ID	2006

Property name	Value
Event name	tmnxDot3OamSdThresholdEvent
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.4
Default severity	minor
Message format string	Port *$ifIndex$ $tmnxDot3OamSdEventLogCleared$ $tmnxDot3OamSdEventLogLocation$* SD fault *$tmnxDot3OamSdEventLogType$ - $tmnxDot3OamSdEventLogValue$* errors exceeded the *$tmnxDot3OamEventLogSdThresholdLo$* error threshold during the *$tmnxDot3OamSdEventLogWindowLo$ $tmnxDot3OamSdEventLogType$* window
Cause	The tmnxDot3OamSdThresholdEvent notification is generated when a local or remote threshold crossing event for signal degradation is detected. A local threshold crossing SD event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates an SD threshold event. This notification should not be sent more than once per second. The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance in the tmnxDot3OamSdEventLogTable. The management entity should periodically check tmnxDot3OamSdEventLogTable to detect any missed events.
Effect	N/A
Recovery	N/A

15.8 tmnxDot3OamThresholdEventClr

Table 416: tmnxDot3OamThresholdEventClr properties

Property name	Value
Application name	EFM_OAM
Event ID	2007
Event name	tmnxDot3OamThresholdEventClr
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.5
Default severity	minor
Message format string	Port *$ifIndex$* cleared *$dot3OamEventLogLocation$* SF fault *$dot3OamEventLogType$ - $dot3OamEventLogValue$* errors

Property name	Value
	exceeded the *$dot3OamEventLogThresholdLo$* error threshold during the *$dot3OamEventLogWindowLo$ $dot3OamEventLogType$* window
Cause	The tmnxDot3OamThresholdEventClr notification is generated when the local or remote signal failure (SF) threshold crossing event is cleared on the port.
Effect	This SF threshold crossing event is no longer a potential cause for the port to restrict user traffic.
Recovery	There is no recovery for this notification.

16 ELMI

16.1 tmnxElmiEVCStatusChangeEvent

Table 417: tmnxElmiEVCStatusChangeEvent properties

Property name	Value
Application name	ELMI
Event ID	2002
Event name	tmnxElmiEVCStatusChangeEvent
SNMP notification prefix and OID	TIMETRA-ELMI-MIB.tmnxElmiNotifications.2
Default severity	minor
Message format string	EVC *$tmnxPortPortID$*: *$tmnxElmiEvcCfgVlanId$* status has changed to *$tmnxElmiEvcCfgStatus$*
Cause	The tmnxElmiEVCStatusChangeEvent notification indicates that the indicated Ethernet Virtual Connection (EVC) has changed its active state (ie. from not active to active). The notification is suppressed when the tmnxElmiIfCfgMode is set to 'none (0)'."
Effect	N/A
Recovery	N/A

16.2 tmnxElmiIfStatusChangeEvent

Table 418: tmnxElmiIfStatusChangeEvent properties

Property name	Value
Application name	ELMI
Event ID	2001
Event name	tmnxElmiIfStatusChangeEvent
SNMP notification prefix and OID	TIMETRA-ELMI-MIB.tmnxElmiNotifications.1
Default severity	minor

Property name	Value
Message format string	ELMI on *$tmnxPortPortID$* has changed status to *$tmnxElmiIfCfg Status$*
Cause	The tmnxElmiStatusChangeEvent notification indicates that the Ethernet LMI Interface has changed state.
Effect	N/A
Recovery	Investigate the cause of the state change.

17 ERING

17.1 tmnxEthRingApsPrvsnClearAlarm

Table 419: tmnxEthRingApsPrvsnClearAlarm properties

Property name	Value
Application name	ERING
Event ID	2003
Event name	tmnxEthRingApsPrvsnClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-RING-MIB.tmnxEthRingApsNotifications.2
Default severity	minor
Message format string	Eth-Ring *$tmnxEthRingIndex$* provisioning mismatch (FOP-PM) cleared
Cause	The tmnxEthRingApsPrvsnClearAlarm is generated when an Ethernet Ring provisioning mismatch is cleared.
Effect	N/A
Recovery	N/A

17.2 tmnxEthRingApsPrvsnRaiseAlarm

Table 420: tmnxEthRingApsPrvsnRaiseAlarm properties

Property name	Value
Application name	ERING
Event ID	2002
Event name	tmnxEthRingApsPrvsnRaiseAlarm
SNMP notification prefix and OID	TIMETRA-ETH-RING-MIB.tmnxEthRingApsNotifications.1
Default severity	minor
Message format string	Eth-Ring *$tmnxEthRingIndex$* provisioning mismatch (FOP-PM) detected: RPL blocked in Node *$node$*

Property name	Value
Cause	The tmnxEthRingApsPrvsnRaiseAlarm is generated when an Ethernet Ring provisioning mismatch is detected. A mismatch occurs when the RPL Owner Node receives one or more No Request R-APS message(s) with RPL Blocked status flag set (NR,RB) and a Node ID that differs from its own.
Effect	N/A
Recovery	Investigate the provisioning mismatch.

17.3 tmnxEthRingPathFwdStateChange

Table 421: tmnxEthRingPathFwdStateChange properties

Property name	Value
Application name	ERING
Event ID	2001
Event name	tmnxEthRingPathFwdStateChange
SNMP notification prefix and OID	TIMETRA-ETH-RING-MIB.tmnxEthRingOprNotifications.1
Default severity	minor
Message format string	Eth-Ring *$tmnxEthRingIndex$* path *$tmnxEthRingPathIndex$* changed fwd state to *$tmnxethRingPathFwdState$*
Cause	The tmnxEthRingPathFwdStateChange is generated when an Ethernet Ring Path changes its forwarding state (tmnxEthRingPathFwdState) from blocked to unblocked or from unblocked to blocked.
Effect	N/A
Recovery	Further investigation required to determine why the forwarding state has changed.

18 ETH_CFM

18.1 dot1agCfmFaultAlarm

Table 422: dot1agCfmFaultAlarm properties

Property name	Value
Application name	ETH_CFM
Event ID	2001
Event name	dot1agCfmFaultAlarm
SNMP notification prefix and OID	IEEE8021-CFM-MIB.dot1agNotifications.1
Default severity	minor
Message format string	MEP *$dot1agCfmMdIndex$*/ *$dot1agCfmMaIndex$*/*$dot1agCfmMep Identifier$* highest defect is now *$dot1agCfmMepHighestPrDefect$*
Cause	A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Whenever a MEP has a persistent defect, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm. If a defect with a higher priority is raised after a Fault Alarm has been issued, another Fault Alarm is issued. The management entity receiving the notification can identify the system from the network source address of the notification, and can identify the MEP reporting the defect by the indices in the OID of the dot1agCfmMepHighest PrDefect variable in the notification: dot1agCfmMdIndex - Also the index of the MEP's Maintenance Domain table entry (dot1agCfm MdTable). dot1agCfmMaIndex - Also an index (with the MD table index) of the MEP's Maintenance Association network table entry (dot1agCfm MaNetTable), and (with the MD table index and component ID) of the MEP's MA component table entry (dot1agCfmMaCompTable). dot1ag CfmMepIdentifier - MEP Identifier and final index into the MEP table (dot1agCfmMepTable). Reference: 802.1ag clause 12.14.7.7
Effect	N/A
Recovery	Investigation is required to determine the cause of the MEP alarm.

18.2 tmnxDot1agCfmMepAisStateChanged

Table 423: tmnxDot1agCfmMepAisStateChanged properties

Property name	Value
Application name	ETH_CFM
Event ID	2006
Event name	tmnxDot1agCfmMepAisStateChanged
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.5
Default severity	minor
Message format string	MEP *$dot1agCfmMdIndex$/ $dot1agCfmMaIndex$/$dot1agCfmMep Identifier$*
Cause	The tmnxDot1agCfmMepAisStateChanged notification is generated when a MEP enters or exits an AIS state.
Effect	N/A
Recovery	N/A

18.3 tmnxDot1agCfmMepCsfStateChanged

Table 424: tmnxDot1agCfmMepCsfStateChanged properties

Property name	Value
Application name	ETH_CFM
Event ID	2009
Event name	tmnxDot1agCfmMepCsfStateChanged
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.8
Default severity	minor
Message format string	Possible messages: • MEP *$dot1agCfmMdIndex$/$dot1agCfmMaIndex$/$dot1agCfmMep Identifier$* is clear of CSF state • MEP *$dot1agCfmMdIndex$/$dot1agCfmMaIndex$/$dot1agCfmMep Identifier$* is in CSF state
Cause	The tmnxDot1agCfmMepCsfStateChanged notification is generated when a MEP enters or exits a CSF state.

Property name	Value
Effect	N/A
Recovery	N/A

18.4 tmnxDot1agCfmMepDMTestComplete

Table 425: tmnxDot1agCfmMepDMTestComplete properties

Property name	Value
Application name	ETH_CFM
Event ID	2005
Event name	tmnxDot1agCfmMepDMTestComplete
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.4
Default severity	minor
Message format string	*$tmnxDot1agCfmMepDelayTestType$* test complete on MEP *$dot1agCfmMdIndex$*/*$dot1agCfmMaIndex$*/*$dot1agCfmMepIdentifier$*: Delay= *$tmnxDot1agCfmMepDelayTestDelay$*us
Cause	The tmnxDot1agCfmMepDMTestComplete notification indicates that a One-Way-Delay-Test (OWDT) frame, or a Two-Way-Delay-Test (TWDT) response was received. For an OWDT frame, traps are raised only when a delay threshold of three seconds is exceeded.
Effect	N/A
Recovery	N/A

18.5 tmnxDot1agCfmMepEthTestComplete

Table 426: tmnxDot1agCfmMepEthTestComplete properties

Property name	Value
Application name	ETH_CFM
Event ID	2004
Event name	tmnxDot1agCfmMepEthTestComplete
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.3

Property name	Value
Default severity	minor
Message format string	eth-test complete on MEP *$dot1agCfmMdIndex$*/*$dot1agCfmMaIndex $*/*$dot1agCfmMepIdentifier$*: Bytes/Failed Bits/CRC Failures= *$tmnx Dot1agCfmMepCurrByteCount$*/*$tmnxDot1agCfmMepCurrFailedBits$*/ *$tmnxDot1agCfmMepCurrCrcFailures$*
Cause	The tmnxDot1agCfmMepEthTestComplete notification indicates that an eth-test has been issued and results are ready. The tmnxDot1ag CfmMepCurrByteCount indicates the number of bytes contained in the frame's Test TLV, and the tmnxDot1agCfmMepCurrFailedBits and tmnxDot1agCfmMepCurrCrcFailures indicate the failure state of the test. A value of Zero (0) for tmnxDot1agCfmMepCurrFailedBits and a value of 'false (2)' for tmnxDot1agCfmMepCurrCrcFailures indicates a successful test.
Effect	N/A
Recovery	N/A

18.6 tmnxDot1agCfmMepFcltyFaultClear

Table 427: tmnxDot1agCfmMepFcltyFaultClear properties

Property name	Value
Application name	ETH_CFM
Event ID	2011
Event name	tmnxDot1agCfmMepFcltyFaultClear
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.10
Default severity	cleared
Message format string	ETH-CFM MEP facility fault cleared *$tmnxDot1agCfmMepFcltyType$ $tmnxDot1agCfmMepFcltyInstance$*
Cause	The tmnxDot1agCfmMepFcltyFaultClear notification is generated when the associated facility MEP has cleared an event affecting the specific tmnxDot1agCfmMepFcltyType tmnxDot1agCfmMepFcltyInstance combination over which it is configured.
Effect	This notification can be used to correlate the ETH_CFM dot1agCfm FaultAlarm event and the related IF-MIB::linkUp notification caused by the facility MEP.
Recovery	N/A

18.7 tmnxDot1agCfmMepFcltyFaultRaise

Table 428: tmnxDot1agCfmMepFcltyFaultRaise properties

Property name	Value
Application name	ETH_CFM
Event ID	2010
Event name	tmnxDot1agCfmMepFcltyFaultRaise
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.9
Default severity	warning
Message format string	ETH-CFM MEP facility fault raised *$tmnxDot1agCfmMepFcltyType$ $tmnxDot1agCfmMepFcltyInstance$*
Cause	The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased.
Effect	This notification can be used to correlate the ETH_CFM dot1agCfm FaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP.
Recovery	Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.

18.8 tmnxDot1agCfmMepLbmTestComplete

Table 429: tmnxDot1agCfmMepLbmTestComplete properties

Property name	Value
Application name	ETH_CFM
Event ID	2002
Event name	tmnxDot1agCfmMepLbmTestComplete
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.1
Default severity	minor
Message format string	loopback test results on MEP *$dot1agCfmMdIndex$*/*$dot1agCfm MaIndex$*/*$dot1agCfmMepIdentifier$* for *$dot1agCfmMepTransmitLbm DestMacAddress$* are available

Property name	Value
Cause	The tmnxDot1agCfmMepLbmTestComplete notification indicates that a loopback test has been issued and results are ready.
Effect	N/A
Recovery	N/A

18.9 tmnxDot1agCfmMepLtmTestComplete

Table 430: tmnxDot1agCfmMepLtmTestComplete properties

Property name	Value
Application name	ETH_CFM
Event ID	2003
Event name	tmnxDot1agCfmMepLtmTestComplete
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.2
Default severity	minor
Message format string	linktrace test results with sequenceNumber *$dot1agCfmMepTransmitLtmSeqNumber$* on MEP *$dot1agCfmMdIndex$*/ *$dot1agCfmMaIndex$*/*$dot1agCfmMepIdentifier$* are now available
Cause	The tmnxDot1agCfmMepLtmTestComplete notification indicates that a linktrace test has been issued and results are ready. The dot1agCfmMepTransmitLtmSeqNumber indicates the Transaction Identifier to use to retrieve the Link-trace results.
Effect	N/A
Recovery	N/A

18.10 tmnxDot1agCfmMepSLMTestComplete

Table 431: tmnxDot1agCfmMepSLMTestComplete properties

Property name	Value
Application name	ETH_CFM
Event ID	2008
Event name	tmnxDot1agCfmMepSLMTestComplete

Property name	Value
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.7
Default severity	minor
Message format string	SLM *$tmnxDot1agCfmMepSlmTestType$* (test-id *$tmnxDot1agCfmMepSlmTestId$*) completed for remote-mep *$tmnxDot1agCfmMepSlmRemoteMepId$* remote MAC *$tmnxDot1agCfmMepSlmRemoteMacAddr$*
Cause	The tmnxDot1agCfmMepSLMTestComplete notification is generated when a one-way or two-way Synthetic Loss Measurement (SLM) test is completed. For one-way SLM test results, tmnxDot1agCfmMepSlmPacketLossOut and tmnxDot1agCfmMepSlmPacketUnack values are fixed at 'zero(0)'.
Effect	N/A
Recovery	N/A

18.11 tmnxDot1agCfmMipEvaluation

Table 432: tmnxDot1agCfmMipEvaluation properties

Property name	Value
Application name	ETH_CFM
Event ID	2007
Event name	tmnxDot1agCfmMipEvaluation
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.6
Default severity	minor
Message format string	Reevaluating MIPs on service *$tmnxDot1agCfmNotifySvcId$* due to virtual MEP configuration
Cause	The tmnxDot1agCfmMipEvaluation notification is generated when a virtual MEP is created or deleted causing MIP reevaluation on the service. On virtual MEP creation, any MIPs in the service will be removed. On virtual MEP deletion, the MIPs are reevaluated.
Effect	N/A
Recovery	N/A

19 ETUN

19.1 tmnxEthTunnelApsCfgClearAlarm

Table 433: tmnxEthTunnelApsCfgClearAlarm properties

Property name	Value
Application name	ETUN
Event ID	2002
Event name	tmnxEthTunnelApsCfgClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.2
Default severity	minor
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* cleared configuration mismatch *$tmnxEthTunnelApsDefectStatus$*
Cause	The tmnxEthTunnelApsCfgClearAlarm is generated when an Ethernet Tunnel Group working and protection configuration mismatch is cleared.
Effect	N/A
Recovery	N/A

19.2 tmnxEthTunnelApsCfgRaiseAlarm

Table 434: tmnxEthTunnelApsCfgRaiseAlarm properties

Property name	Value
Application name	ETUN
Event ID	2001
Event name	tmnxEthTunnelApsCfgRaiseAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.1
Default severity	minor

Property name	Value
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* experiencing configuration mismatch *$tmnxEthTunnelApsDefectStatus$*
Cause	The tmnxEthTunnelApsCfgRaiseAlarm is generated when an Ethernet Tunnel Group working and protection configuration mismatch is detected, at the ETH layer, by detecting the reception of APS protocol from the working transport entity.
Effect	N/A
Recovery	Further investigation required to determine the source of the configuration mismatch.

19.3 tmnxEthTunnelApsNoRspClearAlarm

Table 435: tmnxEthTunnelApsNoRspClearAlarm properties

Property name	Value
Application name	ETUN
Event ID	2006
Event name	tmnxEthTunnelApsNoRspClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.6
Default severity	minor
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* cleared incomplete protection switch (*$tmnxEthTunnelApsDefectStatus$*)
Cause	The tmnxEthTunnelApsNoRspClearAlarm is generated when an Ethernet Tunnel Group no longer experiences an incompletion of protection switching at the ETH layer.
Effect	N/A
Recovery	N/A

19.4 tmnxEthTunnelApsNoRspRaiseAlarm

Table 436: tmnxEthTunnelApsNoRspRaiseAlarm properties

Property name	Value
Application name	ETUN

Property name	Value
Event ID	2005
Event name	tmnxEthTunnelApsNoRspRaiseAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.5
Default severity	minor
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* experiencing incomplete protection switch (*$tmnxEthTunnelApsDefectStatus$*)
Cause	The tmnxEthTunnelApsNoRspRaiseAlarm is generated when an Ethernet Tunnel Group experiences an incompletion of protection switching, at the ETH layer, by comparing the transmitted 'Requested Signal' values and the received 'Bridged Signal' in the APS protocol.
Effect	N/A
Recovery	Further investigation is required to determine the cause of the incomplete protection switch.

19.5 tmnxEthTunnelApsPrvsnClearAlarm

Table 437: tmnxEthTunnelApsPrvsnClearAlarm properties

Property name	Value
Application name	ETUN
Event ID	2004
Event name	tmnxEthTunnelApsPrvsnClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.4
Default severity	minor
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* cleared provisioning mismatch *$tmnxEthTunnelApsDefectStatus$* (*$tmnxEthTunnelApsRxPdu$*/*$tmnxEthTunnelApsTxPdu$*)
Cause	The tmnxEthTunnelApsPrvsnClearAlarm is generated when an Ethernet Tunnel Group provisioning mismatch is cleared.
Effect	N/A
Recovery	N/A

19.6 tmnxEthTunnelApsPrvsnRaiseAlarm

Table 438: tmnxEthTunnelApsPrvsnRaiseAlarm properties

Property name	Value
Application name	ETUN
Event ID	2003
Event name	tmnxEthTunnelApsPrvsnRaiseAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.3
Default severity	minor
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* experiencing provisioning mismatch *$tmnxEthTunnelApsDefectStatus$*: Rx 0x*$tmnxEthTunnelApsRxPdu$* Tx 0x *$tmnxEthTunnelApsTxPdu$*
Cause	The tmnxEthTunnelApsPrvsnRaiseAlarm is generated when an Ethernet Tunnel Group provisioning mismatch is detected, at the ETH layer, by comparing A, B and D bits of the transmitted and received APS protocol. The provision mismatch state is considered as if there is a signal failure on the protection member. This ensures that the working member is kept as active member in the provision mismatch state.
Effect	N/A
Recovery	Further investigation required to determine the source of the provisioning mismatch.

19.7 tmnxEthTunnelApsSwitchoverAlarm

Table 439: tmnxEthTunnelApsSwitchoverAlarm properties

Property name	Value
Application name	ETUN
Event ID	2007
Event name	tmnxEthTunnelApsSwitchoverAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.7
Default severity	minor
Message format string	Eth-Tunnel *$tmnxEthTunnelIndex$* experienced member activity switchover. Path *$tmnxEthTunnelMemberIndex$* is now active.

Property name	Value
Cause	The tmnxEthTunnelApsSwitchoverAlarm is generated when an Ethernet Tunnel Group experiences a member activity switchover. The tmnxEthTunnelMemberPrecedence always specifies the active member.
Effect	N/A
Recovery	N/A

20 FILTER

20.1 tFilterApplyPathProblem

Table 440: tFilterApplyPathProblem properties

Property name	Value
Application name	FILTER
Event ID	2008
Event name	tFilterApplyPathProblem
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.8
Default severity	minor
Message format string	TODO
Cause	The tFilterApplyPathProblem notification is generated when when a problem is encountered for a configured apply-path rule.
Effect	None.
Recovery	No recovery is required.

20.2 tFilterBgpFlowSpecProblem

Table 441: tFilterBgpFlowSpecProblem properties

Property name	Value
Application name	FILTER
Event ID	2007
Event name	tFilterBgpFlowSpecProblem
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.7
Default severity	minor
Message format string	N/A
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

20.3 tFilterEmbeddingOperStateChange

Table 442: tFilterEmbeddingOperStateChange properties

Property name	Value
Application name	FILTER
Event ID	2011
Event name	tFilterEmbeddingOperStateChange
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.11
Default severity	minor
Message format string	The operational state of the embedded filter ID *$tFilterEmbeddedRefEmbeddedFltrId$* in the embedding filter *$tFilterEmbeddedRefFilterType$* ID *$tFilterEmbeddedRefInsertFltrId$* has changed to *$tFilterEmbeddedRefOperState$*.
Cause	This notification may be triggered for the following reasons: 1) An attempt to embed an embedded filter into embedding filter was done. 2) An attempt to recover an embedding that is operationally down was done. 3) An attempt to change the admin state of an embedding was done. 4) The operational state of an embedding has changed to inactive due to lack of resources.
Effect	The effect depends on the new state. If the new state is 'active', the embedding of the filter was successful. If the new state is 'embed FailedNoResources' the embedding was not successful due to lack of resources. If the new state is 'inactive' and the previous state was 'active' then the embedded entries were removed. Otherwise the embedding filter was not changed.
Recovery	If the new state is 'active' or 'inactive', no action is required. If the new state is 'embedFailedNoResources', an attempt to recover the operational state can be done by removal and reapplication of the embedding.

20.4 tFilterEmbedFlowspecOperStateChg

Table 443: tFilterEmbedFlowspecOperStateChg properties

Property name	Value
Application name	FILTER
Event ID	2015
Event name	tFilterEmbedFlowspecOperStateChg
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.14
Default severity	minor
Message format string	The operational state of the embedded flowspec rules of virtual router *$tFilterEmbedFlowspecRtrId$* in the embedding filter *$tFilterEmbed FlowspecFilterType$* ID *$tFilterEmbedFlowspecInsertFltrId$* has changed to *$tFilterEmbedFlowspecOperState$*.
Cause	This notification may be triggered for the following reasons: 1) An attempt to embed a set of flowspec rules into an embedding filter was done. 2) An attempt to recover a flowspec rules embedding that is operationally down was done. 3) An attempt to change the admin state of a flowspec rules embedding was done. 4) The operational state of a flowspec rules embedding has changed to inactive due to lack of resources.
Effect	The effect depends on the new state. If the new state is 'active', the embedding of a set of flowspec rules was successful. If the new state is 'embedFailedNoResources' the embedding was not successful due to lack of resources. If the new state is 'inactive' and the previous state was 'active' then the set of flowspec rules were removed. Otherwise the embedding filter was not changed.
Recovery	If the new state is 'active' or 'inactive', no action is required. If the new state is 'embedFailedNoResources', an attempt to recover the operational state can be done by removal and reapplication of the flowspec rules embedding.

20.5 tFilterEmbedOpenflowOperStateChg

Table 444: tFilterEmbedOpenflowOperStateChg properties

Property name	Value
Application name	FILTER
Event ID	2012

Property name	Value
Event name	tFilterEmbedOpenflowOperStateChg
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.12
Default severity	minor
Message format string	The operational state of the embedded open-flow switch *$tFilterEmbedOpenflowOfsName$* in the embedding filter *$tFilterEmbedOpenflowFilterType$* ID *$tFilterEmbedOpenflowInsertFltrId$* has changed to *$tFilterEmbedOpenflowOperState$*.
Cause	This notification may be triggered for the following reasons: 1) An attempt to embed an open-flow switch into an embedding filter was done. 2) An attempt to recover an open-flow embedding that is operationally down was done. 3) An attempt to change the admin state of an open-flow embedding was done. 4) The operational state of an open-flow embedding has changed to inactive due to lack of resources.
Effect	The effect depends on the new state. If the new state is 'active', the embedding of an open-flow switch was successful. If the new state is 'embedFailedNoResources' the embedding was not successful due to lack of resources. If the new state is 'inactive' and the previous state was 'active' then the open-flow switch entries were removed. Otherwise the embedding filter was not changed.
Recovery	If the new state is 'active' or 'inactive', no action is required. If the new state is 'embedFailedNoResources', an attempt to recover the operational state can be done by removal and reapplication of the open-flow embedding.

20.6 tFilterEmbedVsdOperStateChg

Table 445: tFilterEmbedVsdOperStateChg properties

Property name	Value
Application name	FILTER
Event ID	2016
Event name	tFilterEmbedVsdOperStateChg
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.15
Default severity	minor
Message format string	The operational state of the embedded VSD *$tFilterEmbedVsdFilterType$* filter ID _tmnx_vsd_*$tFilterEmbedVsdEmbeddedFltrId$* in the

Property name	Value
	embedding *$tFilterEmbedVsdFilterType$* filter ID *$tFilterEmbedVsd InsertFltrId$* has changed to *$tFilterEmbedVsdOperState$*.
Cause	This notification may be triggered for the following reasons: 1) An attempt to embed a filter managed by a VSD controller into an embedding filter was done. 2) An attempt to recover an embedding that is operationally down was done. 3) An attempt to change the admin state of an embedding was done. 4) The operational state of an embedding has changed to inactive due to lack of resources.
Effect	The effect depends on the new state. If the new state is 'active', the embedding of a filter managed by a VSD controller was successful. If the new state is 'embedFailedNoResources' the embedding was not successful due to lack of resources. If the new state is 'inactive' and the previous state was 'active' then the embedded entries were removed. Otherwise the embedding filter was not changed.
Recovery	If the new state is 'active' or 'inactive', no action is required. If the new state is 'embedFailedNoResources', an attempt to recover the operational state can be done by removal and reapplication of the embedding.

20.7 tFilterOpenflowRequestRejected

Table 446: tFilterOpenflowRequestRejected properties

Property name	Value
Application name	FILTER
Event ID	2013
Event name	tFilterOpenflowRequestRejected
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	An error was encountered while handlig filter entry *$fltrOpenFlow FlowEntryId$* for the open-flow flowTable *$fltrOpenFlowFlowTable$*. Additional Info: *$fltrOpenFlowProblemDescription$*.
Cause	N/A
Effect	N/A
Recovery	N/A

20.8 tFilterRadSharedFltrAlarmClear

Table 447: tFilterRadSharedFltrAlarmClear properties

Property name	Value
Application name	FILTER
Event ID	2010
Event name	tFilterRadSharedFltrAlarmClear
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.10
Default severity	minor
Message format string	The number of dynamically allocated Radius Shared Filters based on *$tFilterType$ $tFilterId$* has dropped below the threshold of *$tFilter ThresholdReached$*
Cause	The tFilterRadSharedFltrAlarmClear notification is generated when the number of Radius Shared Filters that are dynamically created in the system dropped below to the configured low watermark for the indicated filter.
Effect	The system is working properly, and well within its configured bounds.
Recovery	No recovery is needed.

20.9 tFilterRadSharedFltrAlarmRaised

Table 448: tFilterRadSharedFltrAlarmRaised properties

Property name	Value
Application name	FILTER
Event ID	2009
Event name	tFilterRadSharedFltrAlarmRaised
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.9
Default severity	minor
Message format string	The number of dynamically allocated Radius Shared Filters based on *$tFilterType$ $tFilterId$* has exceeded its threshold of *$tFilterThreshold Reached$*
Cause	The tFilterRadSharedFltrAlarmRaised notification is generated when the number of Radius Shared Filters that are dynamically created in the

Property name	Value
	system increases to the configured high watermark for the indicated filter.
Effect	No direct effect, however the system may run out of filter resources.
Recovery	The way in which dynamically filters are used in the system/network may need to be re-considerd.

20.10 tFilterSubInsFltrEntryDropped

Table 449: tFilterSubInsFltrEntryDropped properties

Property name	Value
Application name	FILTER
Event ID	2006
Event name	tFilterSubInsFltrEntryDropped
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.6
Default severity	warning
Message format string	A request to insert a filter-entry in *$tFilterType$ $tFilterId$* for *$tFilter SubInsSpaceOwner$* has failed - *$tFilterAlarmDescription$*
Cause	A request to insert a filter entry failed.
Effect	The filter may not be working as intended.
Recovery	Actions may be taken depending on the reason of why the insertion failed.

20.11 tFilterSubInsSpaceAlarmCleared

Table 450: tFilterSubInsSpaceAlarmCleared properties

Property name	Value
Application name	FILTER
Event ID	2005
Event name	tFilterSubInsSpaceAlarmCleared
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.5

Property name	Value
Default severity	warning
Message format string	The range of entries reserved in *$tFilterType$ $tFilterId$* for *$tFilterSubInsSpaceOwner$* has fallen below its configured low watermark level *$tFilterThresholdReached$*
Cause	A range of entries in the filter has been reserved (via configuration) to be used for inserting entries by the system. If the number of used entries drops below the (configured) low watermark, this notification is sent.
Effect	The system is working properly, and well within its configured bounds.
Recovery	No recovery is needed.

20.12 tFilterSubInsSpaceAlarmRaised

Table 451: tFilterSubInsSpaceAlarmRaised properties

Property name	Value
Application name	FILTER
Event ID	2004
Event name	tFilterSubInsSpaceAlarmRaised
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.4
Default severity	warning
Message format string	The range of entries reserved in *$tFilterType$ $tFilterId$* for *$tFilterSubInsSpaceOwner$* is filled up to its configured high watermark level *$tFilterThresholdReached$*
Cause	A range of entries in the filter has been reserved (via configuration) to be used for inserting entries by the system. If the number of used entries reaches the (configured) high watermark, this notification is sent.
Effect	If no more entries are available, no more filter entries will be inserted by the system
Recovery	If needed, more entries can be reserved for inserting entries by the system.

20.13 tFilterTmsEvent

Table 452: tFilterTmsEvent properties

Property name	Value
Application name	FILTER
Event ID	2014
Event name	tFilterTmsEvent
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.13
Default severity	minor
Message format string	An event occured on the interface between the filter module and the TMS module. Additional Info: *$tFltrNotifDescription$*.
Cause	The tFilterTmsEvent notification is generated by the systems filter module to report an event related to the Threat Management System (TMS). Receiving the tFilterTmsEvent notification is an indication that the TMS system may not be fully operational.
Effect	None.
Recovery	No recovery is required.

20.14 tIPFilterPBRPacketsDrop

Table 453: tIPFilterPBRPacketsDrop properties

Property name	Value
Application name	FILTER
Event ID	2001
Event name	tIPFilterPBRPacketsDrop
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.1
Default severity	warning
Message format string	Filter *$tIPFilterId$* entry *$tIPFilterParamsIndex$* PBR packets dropped on interface *$tIPFilterParamsForwardNHInterface$* because *$t FilterPBRDropReason$*.
Cause	The tIPFilterPlcyBasedRoutingPacketsDrop event is generated either when the configuration of a forwarding action refers to an invalid/

Property name	Value
	unconfigured next-hop or if the active interface goes down operationally in the process of active filtering.
Effect	The tIPFilterPlcyBasedRoutingPacketsDrop event is generated either when the configuration of a forwarding action refers to an invalid/ unconfigured next-hop or if the active interface goes down operationally in the process of active filtering.
Recovery	No recovery is required.

21 FIREWALL

21.1 aluMcPeerFwBfdSessionClose

Table 454: aluMcPeerFwBfdSessionClose properties

Property name	Value
Application name	FIREWALL
Event ID	2009
Event name	aluMcPeerFwBfdSessionClose
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.9
Default severity	minor
Message format string	Multi-Chassis firewall closed BFD session for peer *$tmnxMcPeerIpAddr $* with source *$tmnxMcPeerSrcIpAddr$*
Cause	The aluMcPeerFwBfdSessionClose notification is generated when the multi-chassis firewall is closing BFD session to the multi-chassis firewall peer.
Effect	N/A
Recovery	N/A

21.2 aluMcPeerFwBfdSessionDown

Table 455: aluMcPeerFwBfdSessionDown properties

Property name	Value
Application name	FIREWALL
Event ID	2011
Event name	aluMcPeerFwBfdSessionDown
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.11
Default severity	minor

Property name	Value
Message format string	Operational state of the BFD session for multi-chassis firewall peer *$tmnxMcPeerIpAddr$* and source *$tmnxMcPeerSrcIpAddr$* is changed to Down
Cause	The aluMcPeerFwBfdSessionDown notification is generated when operational state of the BFD session between the multi-chassis firewall and its peer is changed to 'down'.
Effect	N/A
Recovery	N/A

21.3 aluMcPeerFwBfdSessionOpen

Table 456: aluMcPeerFwBfdSessionOpen properties

Property name	Value
Application name	FIREWALL
Event ID	2008
Event name	aluMcPeerFwBfdSessionOpen
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.8
Default severity	minor
Message format string	Multi-Chassis firewall attempted to open BFD session for peer *$tmnx McPeerIpAddr$* and source *$tmnxMcPeerSrcIpAddr$* with status= *$alu McPeerFwBfdSessionOpenStatus$*
Cause	The aluMcPeerFwBfdSessionOpen notification is generated when the multi-chassis firewall is attempting to open BFD session to the multi-chassis firewall peer.
Effect	N/A
Recovery	N/A

21.4 aluMcPeerFwBfdSessionUp

Table 457: aluMcPeerFwBfdSessionUp properties

Property name	Value
Application name	FIREWALL

Property name	Value
Event ID	2010
Event name	aluMcPeerFwBfdSessionUp
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.10
Default severity	minor
Message format string	Operational state of the BFD session for multi-chassis firewall peer *$tmnxMcPeerIpAddr$* and source *$tmnxMcPeerSrcIpAddr$* is changed to Up
Cause	The aluMcPeerFwBfdSessionUp notification is generated when operational state of the BFD session between the multi-chassis firewall and its peer is changed to 'up'.
Effect	N/A
Recovery	N/A

21.5 aluMcPeerFwElectionMaster

Table 458: aluMcPeerFwElectionMaster properties

Property name	Value
Application name	FIREWALL
Event ID	2014
Event name	aluMcPeerFwElectionMaster
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.14
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* elected Master
Cause	The aluMcPeerFwElectionMaster notification is generated when the multi-chassis firewall node is elected as a Master.
Effect	N/A
Recovery	N/A

21.6 aluMcPeerFwElectionSlave

Table 459: aluMcPeerFwElectionSlave properties

Property name	Value
Application name	FIREWALL
Event ID	2015
Event name	aluMcPeerFwElectionSlave
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.15
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* elected Slave
Cause	The aluMcPeerFwElectionMaster notification is generated when the multi-chassis firewall node is elected as a Slave.
Effect	N/A
Recovery	N/A

21.7 aluMcPeerFwMasterPolicySyncClr

Table 460: aluMcPeerFwMasterPolicySyncClr properties

Property name	Value
Application name	FIREWALL
Event ID	2016
Event name	aluMcPeerFwMasterPolicySyncClr
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.16
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* master policy synchronization flag Cleared
Cause	The aluMcPeerFwMasterPolicySyncClr notification is generated on a multi-chassis firewall Master node before initiating policy synchronization with its peer.
Effect	N/A
Recovery	N/A

21.8 aluMcPeerFwMasterPolicySyncSet

Table 461: aluMcPeerFwMasterPolicySyncSet properties

Property name	Value
Application name	FIREWALL
Event ID	2017
Event name	aluMcPeerFwMasterPolicySyncSet
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.17
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* master policy synchronization flag Set
Cause	The aluMcPeerFwMasterPolicySyncSet notification is generated on a multi-chassis firewall Master node after completing policy synchronization with its Slave peer.
Effect	N/A
Recovery	N/A

21.9 aluMcPeerFwOperDown

Table 462: aluMcPeerFwOperDown properties

Property name	Value
Application name	FIREWALL
Event ID	2012
Event name	aluMcPeerFwOperDown
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.12
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* oper state changed to Down
Cause	The aluMcPeerFwOperDown notification is generated when the multi-chassis firewall detects time-out communicating with the multi-chassis firewall peer.

Property name	Value
Effect	N/A
Recovery	N/A

21.10 aluMcPeerFwOperUp

Table 463: aluMcPeerFwOperUp properties

Property name	Value
Application name	FIREWALL
Event ID	2013
Event name	aluMcPeerFwOperUp
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.13
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* oper state changed to Up
Cause	The aluMcPeerFwOperUp notification is generated when the multi-chassis firewall clears time-out condition in communicating with the multi-chassis firewall peer.
Effect	N/A
Recovery	N/A

21.11 aluMcPeerFwSessionDbSyncClr

Table 464: aluMcPeerFwSessionDbSyncClr properties

Property name	Value
Application name	FIREWALL
Event ID	2020
Event name	aluMcPeerFwSessionDbSyncClr
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.20
Default severity	minor

Property name	Value
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* session database synchronization flag Cleared
Cause	The aluMcPeerFwSessionDbSyncClr notification is generated on a multi-chassis firewall node before initiating Session Database synchronization with its peer.
Effect	N/A
Recovery	N/A

21.12 aluMcPeerFwSessionDbSyncSet

Table 465: aluMcPeerFwSessionDbSyncSet properties

Property name	Value
Application name	FIREWALL
Event ID	2021
Event name	aluMcPeerFwSessionDbSyncSet
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.21
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* session database synchronization flag Set
Cause	The aluMcPeerFwSessionDbSyncSet notification is generated on a multi-chassis firewall node after completing Session Database synchronization with its peer.
Effect	N/A
Recovery	N/A

21.13 aluMcPeerFwSlavePolicySyncClr

Table 466: aluMcPeerFwSlavePolicySyncClr properties

Property name	Value
Application name	FIREWALL
Event ID	2018

Property name	Value
Event name	aluMcPeerFwSlavePolicySyncClr
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.18
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* slave policy synchronization flag Cleared
Cause	The aluMcPeerFwSlavePolicySyncClr notification is generated on a multi-chassis firewall Slave node before initiating policy synchronization with its peer.
Effect	N/A
Recovery	N/A

21.14 aluMcPeerFwSlavePolicySyncSet

Table 467: aluMcPeerFwSlavePolicySyncSet properties

Property name	Value
Application name	FIREWALL
Event ID	2019
Event name	aluMcPeerFwSlavePolicySyncSet
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.19
Default severity	minor
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* slave policy synchronization flag Set
Cause	The aluMcPeerFwSlavePolicySyncSet notification is generated on a multi-chassis firewall Slave node after completing policy synchronization with its Master peer.
Effect	N/A
Recovery	N/A

21.15 aluMcPeerFwSyncStatusChange

Table 468: aluMcPeerFwSyncStatusChange properties

Property name	Value
Application name	FIREWALL
Event ID	2022
Event name	aluMcPeerFwSyncStatusChange
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.22
Default severity	major
Message format string	Multi-Chassis firewall peer *$tmnxMcPeerIpAddr$* syncronization status set to *$aluMcPeerFwSyncStatus$*
Cause	"The aluMcPeerFwSyncStatusChange notification is generated when there is a change of the aluMcPeerFwSyncStatus object."
Effect	N/A
Recovery	N/A

21.16 aluSecPlcyActionPerformed

Table 469: aluSecPlcyActionPerformed properties

Property name	Value
Application name	FIREWALL
Event ID	2001
Event name	aluSecPlcyActionPerformed
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.1
Default severity	major
Message format string	Security policy has been *$subject$*
Cause	Generated when a security policy action is performed.
Effect	N/A
Recovery	N/A

21.17 aluSecSessionHiWtrMrkCrossed

Table 470: aluSecSessionHiWtrMrkCrossed properties

Property name	Value
Application name	FIREWALL
Event ID	2004
Event name	aluSecSessionHiWtrMrkCrossed
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.4
Default severity	major
Message format string	Security session resource alarm detected
Cause	Generated when the concurrent session count exceeds the alarm threshold.
Effect	N/A
Recovery	N/A

21.18 aluSecSessionLoWtrMrkCrossed

Table 471: aluSecSessionLoWtrMrkCrossed properties

Property name	Value
Application name	FIREWALL
Event ID	2005
Event name	aluSecSessionLoWtrMrkCrossed
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.5
Default severity	major
Message format string	Security session resource alarm cleared
Cause	Generated when the concurrent session count crosses the threshold to clear the alarm.
Effect	N/A
Recovery	N/A

21.19 aluSecSessionsExhausted

Table 472: aluSecSessionsExhausted properties

Property name	Value
Application name	FIREWALL
Event ID	2006
Event name	aluSecSessionsExhausted
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.6
Default severity	major
Message format string	All security session resources have been exhausted
Cause	Generated when the concurrent session count reaches the system limit.
Effect	N/A
Recovery	N/A

21.20 aluSecSessionWtrMrkModified

Table 473: aluSecSessionWtrMrkModified properties

Property name	Value
Application name	FIREWALL
Event ID	2003
Event name	aluSecSessionWtrMrkModified
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.3
Default severity	major
Message format string	Security session resource alarm threshold modified
Cause	Generated when the concurrent session alarm thresholds are changed.
Effect	N/A
Recovery	N/A

21.21 aluSecZonePlcyActionPerformed

Table 474: aluSecZonePlcyActionPerformed properties

Property name	Value
Application name	FIREWALL
Event ID	2002
Event name	aluSecZonePlcyActionPerformed
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.2
Default severity	major
Message format string	Security zone %subject% has been *$subject$*
Cause	Generated when a zone security policy action is performed.
Effect	N/A
Recovery	N/A

21.22 aluSecZonePlcyRuleStateChange

Table 475: aluSecZonePlcyRuleStateChange properties

Property name	Value
Application name	FIREWALL
Event ID	2007
Event name	aluSecZonePlcyRuleStateChange
SNMP notification prefix and OID	ALU-SECURITY-MIB.aluSecurityNotification.7
Default severity	major
Message format string	Concurrent security session alarm cleared
Cause	Generated when a rule changes state.
Effect	N/A
Recovery	N/A

22 GMPLS

22.1 vRtrGmplsLspPathStateChange

Table 476: vRtrGmplsLspPathStateChange properties

Property name	Value
Application name	GMPLS
Event ID	2001
Event name	vRtrGmplsLspPathStateChange
SNMP notification prefix and OID	TIMETRA-GMPLS-MIB.tmnxGmplsNotifications.1
Default severity	minor
Message format string	Status of *$lspPathName$* changed administrative state: *$vRtrGmpls LspPathAdminState$*, operational state: *$vRtrGmplsLspPathOperState $*
Cause	A vRtrGmplsLspPathStateChange notification is generated when the operational state of the GMPLS LSP Path changes.
Effect	N/A
Recovery	N/A

23 GSMP

23.1 tmnxAncpEgrRateMonitorEvent

Table 477: tmnxAncpEgrRateMonitorEvent properties

Property name	Value
Application name	GSMP
Event ID	2003
Event name	tmnxAncpEgrRateMonitorEvent
SNMP notification prefix and OID	TIMETRA-GSMP-MIB.tmnxGsmpNotifications.2
Default severity	warning
Message format string	The Egress rate monitor function for the port identified by *$tmnxNotifAncpString$* detects that the scheduler rate *$tmnxNotifAncpPlcyActualRate$* has dropped below the value specified by *$tmnxNotifAncpPolicyName$*
Cause	This notification is generated when the egress rate monitor function for the port identified by tmnxAncpString detects that the scheduler rate has dropped below tmnxAncpPlcyEgrRateMonitor.
Effect	The DLSAM reports (via ANCP) that a subsriber gets less BW than what is currently configured in the system.
Recovery	No recovery is necessary.

23.2 tmnxAncpEgrRateMonitorEventL

Table 478: tmnxAncpEgrRateMonitorEventL properties

Property name	Value
Application name	GSMP
Event ID	2004
Event name	tmnxAncpEgrRateMonitorEventL
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	warning
Message format string	The Egress rate monitor function for the port identified by *$tmnxNotifAncpString$* detects that the scheduler rate *$tmnxNotifAncpPlcyActualRate$* has dropped below the value specified by *$tmnxNotifAncpPolicyName$*
Cause	This notification is generated when the egress rate monitor function for the port identified by tmnxAncpString detects that the scheduler rate has dropped below tmnxAncpPlcyEgrRateMonitor.
Effect	The DLSAM reports (via ANCP) that a subsriber gets less BW than what is currently configured in the system.
Recovery	No recovery is necessary.

23.3 tmnxAncpIngRateMonitorEvent

Table 479: tmnxAncpIngRateMonitorEvent properties

Property name	Value
Application name	GSMP
Event ID	2001
Event name	tmnxAncpIngRateMonitorEvent
SNMP notification prefix and OID	TIMETRA-GSMP-MIB.tmnxGsmpNotifications.1
Default severity	warning
Message format string	The ingress rate monitor function for the port identified by *$tmnxNotifAncpString$* detects that the scheduler rate *$tmnxNotifAncpPlcyActualRate$* has dropped below the value specified by *$tmnxNotifAncpPolicyName$*
Cause	This notification is generated whenever the ingress rate monitor function for the port identified by tmnxAncpString detects that the scheduler rate has dropped below tmnxAncpPlcyIngRateMonitor.
Effect	The DLSAM reports (via ANCP) that a subsriber gets less BW then what is currently configured in the system.
Recovery	No recovery is necessary.

23.4 tmnxAncpIngRateMonitorEventL

Table 480: tmnxAncpIngRateMonitorEventL properties

Property name	Value
Application name	GSMP
Event ID	2002
Event name	tmnxAncpIngRateMonitorEventL
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	The ingress rate monitor function for the port identified by *$tmnxNotifAncpString$* detects that the scheduler rate *$tmnxNotifAncpPlcyActualRate$* has dropped below the value specified by *$tmnxNotifAncpPolicyName$*
Cause	This notification is generated when the ingress rate monitor function for the port identified by tmnxAncpString detects that the scheduler rate has dropped below tmnxAncpPlcyIngRateMonitor.
Effect	The DLSAM reports (via ANCP) that a subsriber gets less BW than what is currently configured in the system.
Recovery	No recovery is necessary.

23.5 tmnxAncpSesRejected

Table 481: tmnxAncpSesRejected properties

Property name	Value
Application name	GSMP
Event ID	2007
Event name	tmnxAncpSesRejected
SNMP notification prefix and OID	TIMETRA-GSMP-MIB.tmnxGsmpNotifications.4
Default severity	warning
Message format string	An incoming ANCP session has been rejected: *$tmnxAncpRejectReason$*

Property name	Value
Cause	The tmnxAncpSesRejected notification is generated when an incoming ANCP session is rejected by the system. Details on why this happened are specified in tmnxAncpRejectReason.
Effect	The ANCP session is rejected.
Recovery	No recovery is necessary.

23.6 tmnxAncpShcvDisabledEvent

Table 482: tmnxAncpShcvDisabledEvent properties

Property name	Value
Application name	GSMP
Event ID	2005
Event name	tmnxAncpShcvDisabledEvent
SNMP notification prefix and OID	TIMETRA-GSMP-MIB.tmnxGsmpNotifications.3
Default severity	warning
Message format string	Subscriber host connectivity verification is disabled for all hosts of the subscriber associated with the *$tmnxNotifAncpString$* when a port-down event was received. AncpPolicy: *$tmnxNotifAncpPolicyName$*
Cause	This notification is generated whenever the SHCV (Subscriber Host Connectivity Verification) is disabled for all hosts of the subscriber associated with the tmnxAncpString when a port-down event was received for the tmnxAncpString.
Effect	The SHCV function is disabled.
Recovery	No recovery is necessary.

23.7 tmnxAncpShcvDisabledEventL

Table 483: tmnxAncpShcvDisabledEventL properties

Property name	Value
Application name	GSMP
Event ID	2006

Property name	Value
Event name	tmnxAncpShcvDisabledEventL
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Subscriber host connectivity verification is disabled for all hosts of the subscriber associated with the *$tmnxNotifAncpString$* when a port-down event was received. AncpPolicy: *$tmnxNotifAncpPolicyName$*
Cause	This notification is generated whenever the SHCV (Subscriber Host Connectivity Verification) is disabled for all hosts of the subscriber associated with the tmnxAncpString when a port-down event was received for the tmnxAncpString."
Effect	The SHCV function is disabled.
Recovery	No recovery is necessary.

23.8 tmnxAncpStringRejected

Table 484: tmnxAncpStringRejected properties

Property name	Value
Application name	GSMP
Event ID	2008
Event name	tmnxAncpStringRejected
SNMP notification prefix and OID	TIMETRA-GSMP-MIB.tmnxGsmpNotifications.5
Default severity	warning
Message format string	An incoming ANCP string rejected: *$tmnxAncpRejectReason$*
Cause	The tmnxAncpStringRejected notification is sent when an incoming ANCP string received on an established ANCP session is rejected by the system. Details on why this happened are specified in tmnxAncp RejectReason.
Effect	The ANCP string is rejected.
Recovery	No recovery is necessary.

24 IGH

24.1 tmnxIfGroupHandlerProtoOprChange

Table 485: tmnxIfGroupHandlerProtoOprChange properties

Property name	Value
Application name	IGH
Event ID	2001
Event name	tmnxIfGroupHandlerProtoOprChange
SNMP notification prefix and OID	TIMETRA-IF-GROUP-HANDLER-MIB.tmnxIfGroupNotifications.1
Default severity	minor
Message format string	IGH *$tmnxIfGroupHandlerIndex$* protocol *$tmnxIfGroupHdlrProto Index$* changed to state *$tmnxIfGroupHdlrProtoStatus$* - admin status: *$tmnxIfGroupHandlerAdminStatus$*, active-links: *$tmnxIfGroupHdlr ProtoActLinks$*, threshold: *$tmnxIfGroupHandlerThreshold$*
Cause	N/A
Effect	N/A
Recovery	N/A

24.2 tmnxIfGroupHdlrMbrProtoOprChange

Table 486: tmnxIfGroupHdlrMbrProtoOprChange properties

Property name	Value
Application name	IGH
Event ID	2002
Event name	tmnxIfGroupHdlrMbrProtoOprChange
SNMP notification prefix and OID	TIMETRA-IF-GROUP-HANDLER-MIB.tmnxIfGroupNotifications.2
Default severity	minor

Property name	Value
Message format string	IGH *$tmnxIfGroupHandlerIndex$* Member *$tmnxPortPortID$* protocol *$tmnxIfGroupHdlrMemberProtoIndex$* changed to state *$tmnxIfGroup HdlrMemberProtoStatus$*
Cause	N/A
Effect	N/A
Recovery	N/A

25 IGMP

25.1 vRtrIgmpGrpIfSapCModeRxQueryMism

Table 487: vRtrIgmpGrpIfSapCModeRxQueryMism properties

Property name	Value
Application name	IGMP
Event ID	2015
Event name	vRtrIgmpGrpIfSapCModeRxQueryMism
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.15
Default severity	minor
Message format string	Mismatch between compatible mode (*$vRtrIgmpGrpIfSapOperVersion $*) for SAP *$sapPortId$* on interface *$vRtrGrpIfIndex$*, IGMP instance *$vRtrID$*, and the IGMP query version (*$vRtrIgmpNotifyQueryVersion $*) received
Cause	A vRtrIgmpGrpIfSapCModeRxQueryMism notification is generated when there is a mismatch between the compatible mode of the IGMP SAP and the version of the received query. It is generated when the SAP is in IGMPv1 compatible mode but it receives a IGMPv2 or IGMPv3 Query. It is also generated when the compatibility mode of the SAP is IGMPv2 but the query received is IGMPv3. sapPortId and sap EncapValue will identify the SAP on which the query is received. vRtr IgmpGrpIfSapOperVersion will indicate the compatibility mode of the SAP and vRtrIgmpNotifyQueryVersion will contain the version of the received query.
Effect	N/A
Recovery	N/A

25.2 vRtrIgmpGrpIfSapMaxGrpsLimExceed

Table 488: vRtrIgmpGrpIfSapMaxGrpsLimExceed properties

Property name	Value
Application name	IGMP

Property name	Value
Event ID	2012
Event name	vRtrIgmpGrpIfSapMaxGrpsLimExceed
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.12
Default severity	minor
Message format string	The number of groups for SAP *$sapPortId$* on interface *$vRtrGrp IfIndex$*, IGMP instance *$vRtrID$*, has exceeded the maximum limit of *$vRtrIgmpGrpIfSapMaxGroups$*
Cause	The vRtrIgmpGrpIfSapMaxGrpsLimExceed event is generated when an attempt is made to configure a group when vRtrIgmpGrpIfSapGroup Count, the number of groups configured on the SAP, is equal to vRtr IgmpGrpIfSapMaxGroups, the maximum number of groups supported on the system.
Effect	N/A
Recovery	N/A

25.3 vRtrIgmpGrpIfSapMaxGrpSrcLimExcd

Table 489: vRtrIgmpGrpIfSapMaxGrpSrcLimExcd properties

Property name	Value
Application name	IGMP
Event ID	2019
Event name	vRtrIgmpGrpIfSapMaxGrpSrcLimExcd
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.19
Default severity	minor
Message format string	The number of groups or sources for SAP *$sapPortId$* on interface *$v RtrGrpIfIndex$*, IGMP instance *$vRtrID$*, has exceeded the maximum limit of *$vRtrIgmpGrpIfSapMaxSources$*
Cause	The vRtrIgmpGrpIfSapMaxGrpSrcLimExcd event is generated when an attempt is made to configure a group source for a group when the number of group sources is equal to vRtrIgmpGrpIfSapMaxGrp Sources, the maximum number of group sources per group supported on the SAP.
Effect	N/A

Property name	Value
Recovery	N/A

25.4 vRtrIgmpGrpIfSapMaxSrcsLimExceed

Table 490: vRtrIgmpGrpIfSapMaxSrcsLimExceed properties

Property name	Value
Application name	IGMP
Event ID	2013
Event name	vRtrIgmpGrpIfSapMaxSrcsLimExceed
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.13
Default severity	minor
Message format string	The number of sources for SAP *$sapPortId$* on interface *$vRtrGrp IfIndex$*, IGMP instance *$vRtrID$*, has exceeded the maximum limit of *$vRtrIgmpGrpIfSapMaxSources$*
Cause	The vRtrIgmpGrpIfSapMaxSrcsLimExceed event is generated when an attempt is made to configure a source for a group when the number of sources for this group is equal to vRtrIgmpGrpIfSapMaxSources, the maximum number of sources per group supported on the system.
Effect	N/A
Recovery	N/A

25.5 vRtrIgmpGrpIfSapMcacPlcyDropped

Table 491: vRtrIgmpGrpIfSapMcacPlcyDropped properties

Property name	Value
Application name	IGMP
Event ID	2014
Event name	vRtrIgmpGrpIfSapMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.14
Default severity	minor

Property name	Value
Message format string	Group *$vRtrIgmpNotifyGrpAddr$* is dropped because of MCAC policy *$vRtrIgmpNotifyMcacPolicyName$* for SAP *$sapPortId$* on interface *$vRtrGrpIfIndex$*, IGMP instance *$vRtrID$*
Cause	The vRtrIgmpGrpIfSapMcacPlcyDropped event is generated when an IGMP group is dropped on a given SAP because of applying a multicast CAC policy given by vRtrIgmpNotifyMcacPolicyName.
Effect	N/A
Recovery	N/A

25.6 vRtrIgmpGrpIfSapRxQueryVerMism

Table 492: vRtrIgmpGrpIfSapRxQueryVerMism properties

Property name	Value
Application name	IGMP
Event ID	2016
Event name	vRtrIgmpGrpIfSapRxQueryVerMism
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.16
Default severity	minor
Message format string	IGMPv*$vRtrIgmpNotifyQueryVersion$* query received for SAP *$sap PortId$* on interface *$vRtrGrpIfIndex$*, IGMP instance *$vRtrID$*, configured as IGMPv*$vRtrIgmpGrpIfSapAdminVersion$*
Cause	A vRtrIgmpGrpIfSapRxQueryVerMism notification is generated when the IGMP host SAP is configured as IGMPv3 but receives a IGMPv1 Query or IGMPv2 General Query on the host. sapPortId and sapEncap Value will identify the SAP on which the query is received. vRtrIgmpGrp IfSapAdminVersion will contain the configured version of the SAP and vRtrIgmpNotifyQueryVersion will contain the version of the received query.
Effect	N/A
Recovery	N/A

25.7 vRtrIgmpHostCModeRxQueryMismatch

Table 493: vRtrIgmpHostCModeRxQueryMismatch properties

Property name	Value
Application name	IGMP
Event ID	2008
Event name	vRtrIgmpHostCModeRxQueryMismatch
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.8
Default severity	minor
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

25.8 vRtrIgmpHostInstantiationFail

Table 494: vRtrIgmpHostInstantiationFail properties

Property name	Value
Application name	IGMP
Event ID	2005
Event name	vRtrIgmpHostInstantiationFail
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.5
Default severity	minor
Message format string	Could not start IGMP on *$vRtrIgmpGrpIfHostLastChangeTime$ - $vRtrIgmpNotifyDescription$*
Cause	The vRtrIgmpHostInstantiationFail event is generated when a host is eligible for running IGMP, but IGMP cannot be started on the host.
Effect	None.
Recovery	Contact Nokia customer service.

25.9 vRtrIgmpHostMaxGrpsLimitExceeded

Table 495: vRtrIgmpHostMaxGrpsLimitExceeded properties

Property name	Value
Application name	IGMP
Event ID	2006
Event name	vRtrIgmpHostMaxGrpsLimitExceeded
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.6
Default severity	minor
Message format string	Could not start IGMP on *$vRtrIgmpGrpIfHostLastChangeTime$ - $vRtrIgmpNotifyDescription$*
Cause	The vRtrIgmpMaxGrpsLimitExceeded event is generated when an attempt is made to configure a group when vRtrIgmpHostGroupCount, the number of groups configured on the PIM interface, is equal to vRtrIgmpHostMaxGroups, the maximum number of groups supported on the system.
Effect	None.
Recovery	Contact Nokia Customer Service.

25.10 vRtrIgmpHostMaxGrpSrcsLimitExcd

Table 496: vRtrIgmpHostMaxGrpSrcsLimitExcd properties

Property name	Value
Application name	IGMP
Event ID	2017
Event name	vRtrIgmpHostMaxGrpSrcsLimitExcd
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.17
Default severity	minor
Message format string	The number of groups or sources configured has exceeded the maximum limit of *$vRtrIgmpHostMaxSources$*
Cause	The vRtrIgmpHostMaxGrpSrcsLimitExcd event is generated when an attempt is made to configure a source for a group when the number of

Property name	Value
	group sources is equal to vRtrIgmpHostMaxGrpSources, the maximum number of group sources per group supported on the host.
Effect	N/A
Recovery	N/A

25.11 vRtrIgmpHostMaxSrcsLimitExceeded

Table 497: vRtrIgmpHostMaxSrcsLimitExceeded properties

Property name	Value
Application name	IGMP
Event ID	2010
Event name	vRtrIgmpHostMaxSrcsLimitExceeded
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.10
Default severity	minor
Message format string	The number of sources configured for a group has exceeded the maximum limit of *$vRtrIgmpHostMaxSources$*
Cause	The vRtrIgmpHostMaxSrcsLimitExceeded event is generated when an attempt is made to configure a source for a group when the number of sources for this group is equal to vRtrIgmpHostMaxSources, the maximum number of sources per group supported on the system.
Effect	N/A
Recovery	N/A

25.12 vRtrIgmpHostMcacPlcyDropped

Table 498: vRtrIgmpHostMcacPlcyDropped properties

Property name	Value
Application name	IGMP
Event ID	2007
Event name	vRtrIgmpHostMcacPlcyDropped

Property name	Value
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.7
Default severity	minor
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

25.13 vRtrIgmpHostQryIntervalConflict

Table 499: vRtrIgmpHostQryIntervalConflict properties

Property name	Value
Application name	IGMP
Event ID	2020
Event name	vRtrIgmpHostQryIntervalConflict
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.20
Default severity	minor
Message format string	TODO
Cause	The vRtrIgmpHostQryIntervalConflict event is generated when one of the IGMP-policy query intervals violates restrictions, we fall back to the node query intervals.
Effect	N/A
Recovery	N/A

25.14 vRtrIgmpHostRxQueryVerMismatch

Table 500: vRtrIgmpHostRxQueryVerMismatch properties

Property name	Value
Application name	IGMP
Event ID	2009

Property name	Value
Event name	vRtrIgmpHostRxQueryVerMismatch
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.9
Default severity	minor
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

25.15 vRtrIgmpIfCModeRxQueryMismatch

Table 501: vRtrIgmpIfCModeRxQueryMismatch properties

Property name	Value
Application name	IGMP
Event ID	2002
Event name	vRtrIgmpIfCModeRxQueryMismatch
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.2
Default severity	warning
Message format string	Mismatch between the interface *$vRtrIfIndex$* compatible mode(*$vRtrIgmpIfOperVersion$*) and the version of the IGMP query (version *$vRtrIgmpNotifyQueryVersion$*) received on the interface
Cause	This notification is generated when there is a mismatch between the compatibility mode of the interface and the version of the IGMP query received on the interace.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

25.16 vRtrIgmpIfRxQueryVerMismatch

Table 502: vRtrIgmpIfRxQueryVerMismatch properties

Property name	Value
Application name	IGMP
Event ID	2001
Event name	vRtrIgmpIfRxQueryVerMismatch
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.1
Default severity	warning
Message format string	IGMPv*$vRtrIgmpNotifyQueryVersion$* query received on interface *$vRtrIfIndex$* configured as IGMPv*$vRtrIgmpIfAdminVersion$*
Cause	The event is generated when the router receives IGMPv1 or IGMPv2 query on an interface which is configured as IGMPv3.
Effect	IGMP interface transitions into IGMPv1 or IGMPv2 compatibility mode.
Recovery	No recovery is necessary.

25.17 vRtrIgmpMaxGrpsLimitExceeded

Table 503: vRtrIgmpMaxGrpsLimitExceeded properties

Property name	Value
Application name	IGMP
Event ID	2003
Event name	vRtrIgmpMaxGrpsLimitExceeded
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.3
Default severity	warning
Message format string	The number of groups configured on the interface *$ifName$* has exceeded the maximum limit of *$vRtrIgmpIfMaxGroups$*
Cause	This notification is generated when the number of groups configured on the interface exceeds the maximum number of groups supported on the system.
Effect	None.
Recovery	Contact Nokia Customer Service.

25.18 vRtrIgmpMaxGrpSrcsLimitExceeded

Table 504: vRtrIgmpMaxGrpSrcsLimitExceeded properties

Property name	Value
Application name	IGMP
Event ID	2018
Event name	vRtrIgmpMaxGrpSrcsLimitExceeded
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.18
Default severity	minor
Message format string	The number of groups or sources configured has exceeded the maximum limit of *$vRtrIgmpIfMaxSources$*
Cause	The vRtrIgmpMaxGrpSrcsLimitExceeded event is generated when an attempt is made to configure a group source for a group when the number of group sources is equal to vRtrIgmpIfMaxGrpSources, the maximum number of group sources per group supported on the interface.
Effect	N/A
Recovery	N/A

25.19 vRtrIgmpMaxSrcsLimitExceeded

Table 505: vRtrIgmpMaxSrcsLimitExceeded properties

Property name	Value
Application name	IGMP
Event ID	2011
Event name	vRtrIgmpMaxSrcsLimitExceeded
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.11
Default severity	minor
Message format string	The number of sources configured for a group has exceeded the maximum limit of *$vRtrIgmpIfMaxSources$*
Cause	The vRtrIgmpMaxSrcsLimitExceeded event is generated when an attempt is made to configure a source for a group when the number

Property name	Value
	of sources for this group is equal to vRtrIgmpHostMaxSources, the maximum number of sources per group supported on the system.
Effect	N/A
Recovery	N/A

25.20 vRtrIgmpMcacPlcyDropped

Table 506: vRtrIgmpMcacPlcyDropped properties

Property name	Value
Application name	IGMP
Event ID	2004
Event name	vRtrIgmpMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.4
Default severity	warning
Message format string	Group *$vRtrIgmpNotifyGrpAddress$* is dropped because of multicast CAC policy *$vRtrIgmpIfMcacPolicyName$* on interface *$ifName$* IGMP instance *$vRtrID$*
Cause	The vRtrIgmpMcacPlcyDropped event is generated when an IGMP group is dropped on a given interface because of applying a multicast CAC policy given by vRtrIgmpIfMcacPolicyName
Effect	None.
Recovery	The Multicast CAC policy must be modified to allow additional groups.

26 IGMP_SNOOPING

26.1 eMplsIgmpSnpgMfibFailure

Table 507: eMplsIgmpSnpgMfibFailure properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2010
Event name	eMplsIgmpSnpgMfibFailure
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgEMplsNotifications.1
Default severity	minor
Message format string	Failing to store an entry in the MFIB table for service $svcId
Cause	The eMplsIgmpSnpgMfibFailure notification is generated when an evpn-mpls binding fails to store an entry in the MFIB table. To resolve this, try to increase the svcTlsMfibTableSize or remove another entry from the MFIB table for this service.
Effect	N/A
Recovery	N/A

26.2 sapIgmpSnpgGrpLimitExceeded

Table 508: sapIgmpSnpgGrpLimitExceeded properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2001
Event name	sapIgmpSnpgGrpLimitExceeded
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.1
Default severity	warning

Property name	Value
Message format string	The number of groups on SAP *$sapEncapValue$* in service *$svcId$* has exceeded the maximum limit of *$sapIgmpSnpgCfgMaxNbrGrps$* - Dropping group *$alxIgmpSnpgGroupAddress$*
Cause	The sapIgmpSnpgGrpLimitExceeded notification is generated when an IGMP group is dropped on a given SAP because a user configurable upper limit given by sapIgmpSnpgCfgMaxNbrGrps is reached.
Effect	None.
Recovery	Investigate the cause of the excessive groups.

26.3 sapIgmpSnpgGrpSrcLimitExceeded

Table 509: sapIgmpSnpgGrpSrcLimitExceeded properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2009
Event name	sapIgmpSnpgGrpSrcLimitExceeded
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.5
Default severity	minor
Message format string	The number of groups or sources on SAP *$sapEncapValue$* in service *$svcId$* has exceeded the maximum limit of *$sapIgmpSnpgCfgMaxNbr Srcs$* - Dropping source *$alxIgmpSnpgSourceAddress$* for group *$alx IgmpSnpgGroupAddress$*
Cause	The sapIgmpSnpgGrpSrcLimitExceeded notification is generated when an IGMP group or source is dropped dropped on a given SAP because a user configurable upper limit given by sapIgmpSnpgCfgMaxNbrGrp Srcs is reached.
Effect	The specified S,G was not added.
Recovery	Investigate the cause of the excessive sources.

26.4 sapIgmpSnpgMcacPlcyDropped

Table 510: sapIgmpSnpgMcacPlcyDropped properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2002
Event name	sapIgmpSnpgMcacPlcyDropped
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.2
Default severity	warning
Message format string	Group *$alxIgmpSnpgGroupAddress$* is dropped because of multicast CAC policy *$sapIgmpSnpgCfgMcacPolicyName$* on SAP *$sapEncap Value$* in service *$svcId$*
Cause	The sapIgmpSnpgMcacPlcyDropped notification is generated when an IGMP group is dropped on a given SAP because of applying a multicast CAC policy given by sapIgmpSnpgCfgMcacPolicyName.
Effect	None.
Recovery	Investigate the cause of the excessive groups.

26.5 sapIgmpSnpgMcsFailure

Table 511: sapIgmpSnpgMcsFailure properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2005
Event name	sapIgmpSnpgMcsFailure
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.3
Default severity	warning
Message format string	Group *$alxIgmpSnpgGroupAddress$* on SAP *$sapEncapValue$* in service *$svcId$* could not be synced to MCS - *$alxIgmpSnpgMcs FailureReason$*
Cause	The sapIgmpSnpgMcsFailure notification is generated when an IGMP group on a given SAP could not be synced to the MCS (multi-chassis synchronization) database.

Property name	Value
Effect	Synchronization between chassis has been lost.
Recovery	No recovery is required.

26.6 sapIgmpSnpgSrcLimitExceeded

Table 512: sapIgmpSnpgSrcLimitExceeded properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2006
Event name	sapIgmpSnpgSrcLimitExceeded
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.1
Default severity	warning
Message format string	The number of sources for group *$alxIgmpSnpgGroupAddress$* on SAP *$sapEncapValue$* in service *$svcId$* has exceeded the maximum limit of *$sapIgmpSnpgCfgMaxNbrSrcs$* - Dropping source *$alxIgmp SnpgSourceAddress$* for group *$alxIgmpSnpgGroupAddress$*
Cause	The sapIgmpSnpgSrcLimitExceeded notification is generated when an IGMP source is dropped on a given SAP because a user configurable upper limit given by sapIgmpSnpgCfgMaxNbrSrcs is reached.
Effect	The specified S,G was not added.
Recovery	Investigate the cause of the excessive sources.

26.7 sdpBndIgmpSnpgGrpLimitExceeded

Table 513: sdpBndIgmpSnpgGrpLimitExceeded properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2003
Event name	sdpBndIgmpSnpgGrpLimitExceeded
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSdpBndNotifications.1

Property name	Value
Default severity	warning
Message format string	The number of groups on SDP Bind *$sdpBindId$* in service *$svcId$* has exceeded the maximum limit of *$sdpBndIgmpSnpgCfgMaxNbr Grps$* - Dropping group *$alxIgmpSnpgGroupAddress$*
Cause	The sdpBndIgmpSnpgGrpLimitExceeded notification is generated when an IGMP group is dropped on a given SDP bind because a user configurable upper limit given by sdpBndIgmpSnpgCfgMaxNbrGrps is reached.
Effect	None.
Recovery	Investigate the cause of the excessive groups.

26.8 sdpBndIgmpSnpgGrpSrcLimitExceed

Table 514: sdpBndIgmpSnpgGrpSrcLimitExceed properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2008
Event name	sdpBndIgmpSnpgGrpSrcLimitExceed
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSdpBndNotifications.4
Default severity	minor
Message format string	The number of groups or sources on SDP Bind *$sdpBindId$* in service *$svcId$* has exceeded the maximum limit of *$sdpBndIgmpSnpgCfgMax NbrSrcs$* - Dropping source *$alxIgmpSnpgSourceAddress$* for group *$alxIgmpSnpgGroupAddress$*
Cause	The sdpBndIgmpSnpgGrpSrcLimitExceed notification is generated when an IGMP group or source is dropped on a given SDP Bind because a user configurable upper limit given by sdpBndIgmpSnpgCfg MaxNbrGrpSrcs is reached.
Effect	The specified S,G was not added.
Recovery	Investigate the cause of the excessive sources.

26.9 sdpBndIgmpSnpgMcacPlcyDropped

Table 515: sdpBndIgmpSnpgMcacPlcyDropped properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2004
Event name	sdpBndIgmpSnpgMcacPlcyDropped
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSdpBndNotifications.2
Default severity	warning
Message format string	Group *$alxIgmpSnpgGroupAddress$* is dropped because of multicast CAC policy *$sdpBndIgmpSnpgCfgMcacPolicyName$* on SDP Bind *$sdpBindId$* in service *$svcId$*
Cause	The sdpBndIgmpSnpgMcacPlcyDropped notification is generated when an IGMP group is dropped on a given SDP bind because of applying a multicast CAC policy given by sdpBndIgmpSnpgCfgMcacPolicyName.
Effect	None.
Recovery	Investigate the cause of the excessive groups.

26.10 sdpBndIgmpSnpgSrcLimitExceeded

Table 516: sdpBndIgmpSnpgSrcLimitExceeded properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2007
Event name	sdpBndIgmpSnpgSrcLimitExceeded
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSdpBndNotifications.1
Default severity	warning
Message format string	The number of sources for group *$alxIgmpSnpgGroupAddress$* on SDP Bind *$sdpBindId$* in service *$svcId$* has exceeded the maximum limit of *$sdpBndIgmpSnpgCfgMaxNbrSrcs$* - Dropping source *$alx IgmpSnpgSourceAddress$* for group *$alxIgmpSnpgGroupAddress$*
Cause	The sdpBndIgmpSnpgSrcLimitExceeded notification is generated when an IGMP source is dropped on a given SDP Bind because a user

Property name	Value
	configurable upper limit given by sdpBndIgmpSnpgCfgMaxNbrSrcs is reached.
Effect	The specified S,G was not added.
Recovery	Investigate the cause of the excessive sources.

27 IP

27.1 clearRTMError

Table 517: clearRTMError properties

Property name	Value
Application name	IP
Event ID	2001
Event name	clearRTMError
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Could not flush IOMs *$iomList$* because 'clear' failed
Cause	A failure has occured with communications with the associated IOM.
Effect	N/A
Recovery	Contact the Nokia Customer Service.

27.2 fibAddFailed

Table 518: fibAddFailed properties

Property name	Value
Application name	IP
Event ID	2005
Event name	fibAddFailed
SNMP notification prefix and OID	N/A
Default severity	major
Message format string	FIB add failed for VRF *$vRtrID$* prefix *$prefix$*
Cause	FIB resources have been exhausted.

Property name	Value
Effect	Additional routing information can not be added to the forwarding table.
Recovery	Further investigation is required to determine why the IP route table entry could not be added.

27.3 ipAnyDuplicateAddress

Table 519: ipAnyDuplicateAddress properties

Property name	Value
Application name	IP
Event ID	2010
Event name	ipAnyDuplicateAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	State changed from *$stateFrom$* to *$stateTo$* for IP address *$ip Address$* sent from ethernet address *$macAddress$* for interface *$int Name$*
Cause	Another system on the subnet has the same IP address.
Effect	Communications to or from systems with duplicate IP addresses may not be possible.
Recovery	The duplicate IP address should be removed.

27.4 ipArpBadInterface

Table 520: ipArpBadInterface properties

Property name	Value
Application name	IP
Event ID	2007
Event name	ipArpBadInterface
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Message format string	ARP request for *$ipAddress$* received on *$interface1$*, expected *$interface2$*
Cause	ARP request received on the wrong interface.
Effect	Communications to or from systems with duplicate IP addresses may not be possible.
Recovery	Further investigation is required, a possible L2 loop could exist.

27.5 ipArpDuplicateIpAddress

Table 521: ipArpDuplicateIpAddress properties

Property name	Value
Application name	IP
Event ID	2008
Event name	ipArpDuplicateIpAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	duplicate IP address *$ipAddress$* with *$macAddress$* on interface *$interface$*
Cause	Another system on the subnet has the same IP address.
Effect	Communications to or from systems with duplicate IP addresses may not be possible.
Recovery	Duplicate IP addresses must be corrected by changing the IP address on one of the systems.

27.6 ipArpDuplicateMacAddress

Table 522: ipArpDuplicateMacAddress properties

Property name	Value
Application name	IP
Event ID	2009

Property name	Value
Event name	ipArpDuplicateMacAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	duplicate MAC address *$macAddress$* with *$ipAddress$* on interface *$interface$*
Cause	Another system or host on the ethernet segment has the same ethernet MAC address.
Effect	Communications to or from systems with duplicate MAC addresses may not be possible.
Recovery	The duplicate MAC address should be removed.

27.7 ipArpInfoOverwritten

Table 523: ipArpInfoOverwritten properties

Property name	Value
Application name	IP
Event ID	2004
Event name	ipArpInfoOverwritten
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	ARP information overwritten for *$ipAddress$* by *$macAddress$*
Cause	ARP information has been updated.
Effect	None.
Recovery	No recovery is required.

27.8 ipDuplicateAddress

Table 524: ipDuplicateAddress properties

Property name	Value
Application name	IP
Event ID	2003
Event name	ipDuplicateAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Duplicate IP address *$ipAddress$* sent from ethernet address *$mac Address$*
Cause	Another system or host on the ethernet subnet has the same IP address.
Effect	Communications to or from systems with duplicate IP addresses may not be possible.
Recovery	Duplicate IP addresses must be corrected by changing the IP address on one of the systems.

27.9 ipEtherBroadcast

Table 525: ipEtherBroadcast properties

Property name	Value
Application name	IP
Event ID	2002
Event name	ipEtherBroadcast
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Invalid ethernet (broadcast) address for IP address *$ipAddress$*
Cause	Misconfigured or misbehaving host is sending the incorrect MAC address.
Effect	Communications to or from systems with invalid MAC addresses may not be possible.

Property name	Value
Recovery	Further investigation required on the host.

27.10 qosNetworkPolicyMallocFailed

Table 526: qosNetworkPolicyMallocFailed properties

Property name	Value
Application name	IP
Event ID	2006
Event name	qosNetworkPolicyMallocFailed
SNMP notification prefix and OID	N/A
Default severity	major
Message format string	Qos Network Policy malloc failed in *$function$*
Cause	QoS Network policies have been exhausted.
Effect	Additional QoS Network policies can not be configured.
Recovery	Contact the Nokia Customer Service.

28 IPSEC

28.1 aluIPsecTunnelAuthFailure

Table 527: aluIPsecTunnelAuthFailure properties

Property name	Value
Application name	IPSEC
Event ID	2014
Event name	aluIPsecTunnelAuthFailure
SNMP notification prefix and OID	ALU-IPSEC-MIB.aluIPsecNotifications.1
Default severity	minor
Message format string	Tunnel $aluIPsecTunnelName failed authentication.
Cause	The trap aluIPsecTunnelAuthFailure is sent when there is an authentication failure to bring up an IPsec tunnel.
Effect	The IPsec tunnel does not becom in service.
Recovery	Correct authentication parameters mismatch.

28.2 aluIPsecTunnelMalformedMessage

Table 528: aluIPsecTunnelMalformedMessage properties

Property name	Value
Application name	IPSEC
Event ID	2016
Event name	aluIPsecTunnelMalformedMessage
SNMP notification prefix and OID	ALU-IPSEC-MIB.aluIPsecNotifications.3
Default severity	minor
Message format string	Received a malformed message for tunnel $aluIPsecTunnelName.

Property name	Value
Cause	The trap aluIPsecTunnelMalformedMessage is sent when there is an IKE message with a malformed message or missing payload.
Effect	The IPsec tunnel does not becom in service.
Recovery	A mismatched configuration between IPsec tunnel endpoints can cause the responder to send an IKE message with missing or unexpected payloads. Check IPsec logs on both ends and correct any issues.

28.3 aluIPsecTunnelMalformedPayload

Table 529: aluIPsecTunnelMalformedPayload properties

Property name	Value
Application name	IPSEC
Event ID	2015
Event name	aluIPsecTunnelMalformedPayload
SNMP notification prefix and OID	ALU-IPSEC-MIB.aluIPsecNotifications.2
Default severity	minor
Message format string	Received a malformed payload for tunnel $aluIPsecTunnelName.
Cause	The trap aluIPsecTunnelMalformedPayload is sent when there is an IKE message with a malformed payload.
Effect	The IPsec tunnel does not becom in service.
Recovery	A mismatched configuration between IPsec tunnel endpoints can cause the responder to send an IKE message with missing or unexpected payloads. Check IPsec logs on both ends and correct any issues.

28.4 aluIPsecTunnelTransformMismatch

Table 530: aluIPsecTunnelTransformMismatch properties

Property name	Value
Application name	IPSEC
Event ID	2017
Event name	aluIPsecTunnelTransformMismatch

Property name	Value
SNMP notification prefix and OID	ALU-IPSEC-MIB.aluIPsecNotifications.4
Default severity	minor
Message format string	Tunnel $aluIPsecTunnelName has mismatched transform.
Cause	The trap aluIPsecTurnnelTransformMismatch is sent when there is an mismatch between IPSec transforms.
Effect	The IPsec tunnel does not becom in service.
Recovery	A mismatched configuration between IPsec tunnel endpoints could be the cause. Check IPsec logs on both ends and correct any issues.

28.5 tIPsecBfdIntfSessStateChgd

Table 531: tIPsecBfdIntfSessStateChgd properties

Property name	Value
Application name	IPSEC
Event ID	2003
Event name	tIPsecBfdIntfSessStateChgd
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.3
Default severity	minor
Message format string	BFD session on service *$tIPsecNotifBfdIntfSvcId$* interface *$tIPsecNotifBfdIntfIfName$* to peer *$tIPsecNotifBfdIntfDestIp$* changed state to *$tIPsecNotifBfdIntfSessState$*.
Cause	The operational state of a BFD session of the IPsec instance changed.
Effect	None.
Recovery	No recovery is necessary.

28.6 tIPsecRadAcctPlcyFailure

Table 532: tIPsecRadAcctPlcyFailure properties

Property name	Value
Application name	IPSEC

Property name	Value
Event ID	2004
Event name	tIPsecRadAcctPlcyFailure
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.4
Default severity	minor
Message format string	Failed to send RADIUS accounting request for policy *$tIPsecRadAcctPlcyName$* due to: *$tIPsecRadAcctPlcyFailReason$*
Cause	The tIPsecRadAcctPlcyFail notification is generated when a RADIUS accounting request was not sent out successfully to any of the RADIUS servers in the indicated accounting policy.
Effect	The RADIUS server may not receive the accounting information.
Recovery	Depending on the reason indicated as per 'tIPsecRadAcctPlcyFailReason', 'tIPsecRadAcctPlcyTable' configuration may need to be changed.

28.7 tIPsecRUSAFailToAddRoute

Table 533: tIPsecRUSAFailToAddRoute properties

Property name	Value
Application name	IPSEC
Event ID	2002
Event name	tIPsecRUSAFailToAddRoute
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.2
Default severity	warning
Message format string	IPsec Remote-User tunnel *$tIPsecRUTnlInetAddress $*:*$tIPsecRUTnlPort$* failed to add route to *$tIPsecRUSARemAddr$*/*$tIPsecRUSARemAPrefLen$* because *$tIPsecNotifReason$*.
Cause	The event is generated when creation of a remote-user tunnel fails.
Effect	None.
Recovery	No recovery is necessary.

28.8 tIPsecRuTnlEncapIpMtuTooSmall

Table 534: tIPsecRuTnlEncapIpMtuTooSmall properties

Property name	Value
Application name	IPSEC
Event ID	2007
Event name	tIPsecRuTnlEncapIpMtuTooSmall
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.7
Default severity	warning
Message format string	Addition of tunnel encapsulation at IPsec remote user tunnel on SAP: *$sapEncapValue$*, service:*$svcId$* for IP address *$tIPsecNotifRUTnlInetAddress$*: *$tIPsecNotifRUTnlPort$* with configured MTU of *$tIPsecNotifConfigIpMtu$*, having encapsulated MTU of *$tIPsecNotifConfigEncapIpMtu$* has an overhead of *$tIPsecNotifEncapOverhead$*.
Cause	The tIPsecRuTnlEncapIpMtuTooSmall notification is generated when the addition of tunnel encapsulation to a packet at or near the IPsec remote user tunnel's configured IP MTU may cause it to exceed the tunnel's configured encapsulated IP MTU.
Effect	The pre-encapsulated packet may be fragmented, and will require reassembly by the tunnel remote endpoint, causing a performance impact.
Recovery	Configured IP MTU and/or encapsulated IP MTU may need to be changed depending on the size of the encapsulation overhead as indicated in 'tIPsecNotifEncapOverhead', and the transmission capabilities of the tunnel's transport network.

28.9 tIPsecRUTnlFailToCreate

Table 535: tIPsecRUTnlFailToCreate properties

Property name	Value
Application name	IPSEC
Event ID	2001
Event name	tIPsecRUTnlFailToCreate
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.1
Default severity	warning

Property name	Value
Message format string	Creation of an IPsec Remote-User tunnel *$tIPsecNotifRUTnlInet Address$*:*$tIPsecNotifRUTnlPort$* on SAP: *$sapEncapValue$*, service:*$svcId$* failed because *$tIPsecNotifReason$*.
Cause	The event is generated when creation of a remote-user tunnel fails.
Effect	None.
Recovery	No recovery is necessary.

28.10 tIPsecRUTnlRemoved

Table 536: tIPsecRUTnlRemoved properties

Property name	Value
Application name	IPSEC
Event ID	2013
Event name	tIPsecRUTnlRemoved
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.13
Default severity	minor
Message format string	IPsec Remote-User tunnel *$tIPsecNotifRUTnlInetAddress$*:*$tIPsec NotifRUTnlPort$* on SAP: *$sapEncapValue$*, service:*$svcId$* was removed because *$tIPsecNotifReason$*.
Cause	A tIPsecRUTnlRemoved notification is generated when a remote-user tunnel is removed under certain reasons, which are indicated by tIPsec NotifReason (e.g., failed to renew private address lease with DHCP server).
Effect	The IPsec tunnel becomes operationally out of service.
Recovery	N/A

28.11 tIPSecTrustAnchorPrfOprChg

Table 537: tIPSecTrustAnchorPrfOprChg properties

Property name	Value
Application name	IPSEC

Property name	Value
Event ID	2005
Event name	tIPSecTrustAnchorPrfOprChg
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.5
Default severity	minor
Message format string	*$tIPsecTrustAnchorCAProfDown$* of the configured trust-anchors in profile *$tIPsecTrustAnchorProfName$* are not operational
Cause	The tIPSecTrustAnchorPrfOprChg notification is generated when not all of the trust-anchors in a profile are operational.
Effect	Authentication of tunnels configured with the trust-anchor-profile will fail if the trusted CA (Certificate Authority) in the certificate chain is not operational.
Recovery	Bring the trusted CA-profile operational up.

28.12 tIPsecTunnelEncapIpMtuTooSmall

Table 538: tIPsecTunnelEncapIpMtuTooSmall properties

Property name	Value
Application name	IPSEC
Event ID	2006
Event name	tIPsecTunnelEncapIpMtuTooSmall
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.6
Default severity	warning
Message format string	Addition of tunnel encapsulation at IPsec static tunnel *$tIPsec NotifIPsecTunnelName$* on SAP:*$sapEncapValue$*, service: *$svcId$* with configured MTU of *$tIPsecNotifConfigIpMtu$*, having encapsulated MTU of *$tIPsecNotifConfigEncapIpMtu$* has an overhead of *$tIPsec NotifEncapOverhead$*
Cause	The tIPsecTunnelEncapIpMtuTooSmall notification is generated when the addition of tunnel encapsulation to a packet at or near the IPsec static tunnel's configured IP MTU may cause it to exceed the tunnel's configured encapsulated IP MTU.

Property name	Value
Effect	The pre-encapsulated packet may be fragmented, and will require reassembly by the tunnel remote endpoint, causing a performance impact.
Recovery	Configured IP MTU and/or encapsulated IP MTU may need to be changed depending on the size of the encapsulation overhead as indicated in 'tIPsecNotifEncapOverhead', and the transmission capabilities of the tunnel's transport network.

28.13 tmnxIPsecGWOperStateChange

Table 539: tmnxIPsecGWOperStateChange properties

Property name	Value
Application name	IPSEC
Event ID	2012
Event name	tmnxIPsecGWOperStateChange
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.12
Default severity	minor
Message format string	Operational state change for IPsec Gateway *$tmnxIPsecGWName $* on service *$svcId$* and SAP *$sapEncapValue$*, admin state: *$tmnxIPsecGWAdminState$*, oper state: *$tmnxIPsecGWOperState$*, oper flags: *$tmnxIPsecGWOperFlags$*
Cause	The tmnxIPsecGWOperStateChange notification is generated when there is a state change in tmnxIPsecGWOperState for an IPsec gateway.
Effect	When the value of tmnxIPsecGWOperState is 'outOfService (3)', the IPesc gateway is operationally down and it is not ready to negotiate IKE sessions with remote clients. When the value of tmnxIPsecGWOperState is 'inService (2)', the IPsec gateway is operationally up. When the value of tmnxIPsecGWOperState is 'hold (5)', the IPsec gateway is operationally up but not ready to negotiate any new IKE sessions with remote clients.
Recovery	Please refer to tmnxIPsecGWOperFlags for information on why the gateway is operationally down.

28.14 tmnxIPsecTunnelOperStateChange

Table 540: tmnxIPsecTunnelOperStateChange properties

Property name	Value
Application name	IPSEC
Event ID	2011
Event name	tmnxIPsecTunnelOperStateChange
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.11
Default severity	minor
Message format string	Operational state change for IPsec Tunnel *$tmnxIPsecTunnelName $* on service *$svcId$* and SAP *$sapEncapValue$*, admin state: *$tmnxIPsecTunnelAdminState$*, oper state: *$tmnxIPsecTunnelOper State$*, oper flags: *$tmnxIPsecTunnelOperFlags$*
Cause	The tmnxIPsecTunnelOperStateChange notification is generated when there is a change in tmnxIPsecTunnelOperState for an IPsec tunnel.
Effect	When the value of tmnxIPsecTunnelOperState is 'outOfService (3)', the IPesc tunnel is operationally down and traffic arriving at the tunnel endpoints will not be encapsulated and transported. When the value of tmnxIPsecTunnelOperState is 'inService (2)', the IPsec tunnel is operationally up. When the value of tmnxIPsecGWOperState is 'hold (5)', the IPsec tunnel is operationally up but not ready to re-establish the connection until the conditions indicated in the tmnxIPsecTunnel OperFlags are cleared.
Recovery	Please refer to tmnxIPsecTunnelOperFlags for information on why the tunnel is operationally down.

28.15 tmnxSecNotifCmptedCertChnChngd

Table 541: tmnxSecNotifCmptedCertChnChngd properties

Property name	Value
Application name	IPSEC
Event ID	2009
Event name	tmnxSecNotifCmptedCertChnChngd
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.9
Default severity	minor

Property name	Value
Message format string	Certificate chain changed to *$tIPsecNotifCaProfNames$* in cert-profile *$tIPsecNotifCertProfileName$* entry *$tIPsecNotifCertProfEntryId$*
Cause	The tmnxSecNotifCmptedCertChnChngd notification is generated when a computed certificate chain is changed due to a dependent CA profile being changed and brought into service.
Effect	The hash of the recomputed certificate chain, if changed, will be used for choosing cert-profile entry during new IPsec tunnel establishment.
Recovery	If the changed CA certificate is used as a trust-anchor at the peer, then the certificate should be updated at the peer as well to ensure correct cert-profile entry selection.

28.16 tmnxSecNotifCmptedCertHashChngd

Table 542: tmnxSecNotifCmptedCertHashChngd properties

Property name	Value
Application name	IPSEC
Event ID	2008
Event name	tmnxSecNotifCmptedCertHashChngd
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.8
Default severity	minor
Message format string	Hash of certificate chain changed in cert-profile *$tIPsecNotifCertProfile Name$* entry *$tIPsecNotifCertProfEntryId$* due to CA profile *$tIPsec NotifCaProfNames$*
Cause	The tmnxSecNotifCmptedCertHashChngd notification is generated when the hash of a certificate chain is changed.
Effect	The hash of the recomputed certificate chain will be used for choosing cert-profile entry during new IPsec tunnel establishment.
Recovery	If the changed CA certificate is used as a trust-anchor at the peer, then the certificate should be updated at the peer as well to ensure correct cert-profile entry selection.

28.17 tmnxSecNotifSendChnNotInCmptChn

Table 543: tmnxSecNotifSendChnNotInCmptChn properties

Property name	Value
Application name	IPSEC
Event ID	2010
Event name	tmnxSecNotifSendChnNotInCmptChn
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.10
Default severity	minor
Message format string	Send-chain CA profile *$tIPsecNotifCaProfNames$* not in the computed certificate chain of cert-profile *$tIPsecNotifCertProfileName$* entry *$tIPsecNotifCertProfEntryId$*
Cause	The tmnxSecNotifSendChnNotInCmptChn notification is generated when a CA profile not belonging to the computed certificate chain is added to the send-chain of a cert-profile entry, or the certificate chain is changed such that a CA-profile in the send-chain is no longer a member of the chain.
Effect	The CA certificate(s) to be sent to the peer is not a member of the certificate chain that is requested by the peer for new IPsec tunnel establishment.
Recovery	Replace the send-chain CA profile that is not in the certificate chain with one that is.

29 ISIS

29.1 tmnxIsisAdjacencyChange

Table 544: tmnxIsisAdjacencyChange properties

Property name	Value
Application name	ISIS
Event ID	2045
Event name	tmnxIsisAdjacencyChange
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.17
Default severity	warning
Message format string	Adjacency status changed to *$isisISAdjState$* for interface: *$vRtr IfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, LSP-id: *$vRtrIsis TrapLSPIDString$*
Cause	The tmnxIsisAdjacencyChange notification is sent when an adjacency changes state, entering or leaving state up. The first 6 bytes of the tmnxIsisNotifTrapLSPID are the SystemID of the adjacent IS. The isisISAdjState is the new state of the adjacency.
Effect	No effect.
Recovery	No recovery is necessary.

29.2 tmnxIsisAdjBfdSessionSetupFail

Table 545: tmnxIsisAdjBfdSessionSetupFail properties

Property name	Value
Application name	ISIS
Event ID	2062
Event name	tmnxIsisAdjBfdSessionSetupFail
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.34
Default severity	warning

Property name	Value
Message format string	BFD session setup failed with reason *$tmnxIsisBfdSessSetupFail Reason$* for interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystem Level$*, LSP-id: *$tmnxIsisNotifTrapLSPIDString$*
Cause	The tmnxIsisAdjBfdSessionSetupFail notification is sent when BFD session setup fails. The first 6 bytes of the tmnxIsisNotifTrapLSPID are the SystemID of the adjacent IS.
Effect	The system can not setup the BFD session.
Recovery	Depending on the tmnxIsisBfdSessSetupFailReason, recovery can be possible. Check the BFD configuration to recover.

29.3 tmnxIsisAdjRestartStatusChange

Table 546: tmnxIsisAdjRestartStatusChange properties

Property name	Value
Application name	ISIS
Event ID	2047
Event name	tmnxIsisAdjRestartStatusChange
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.19
Default severity	warning
Message format string	Adjacency graceful restart status changed to *$tmnxIsisISAdjRestart Status$* for interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystem Level$*
Cause	The tmnxIsisAdjRestartStatusChange notification is sent when an adjancency's graceful restart status changes. The tmnxIsisISAdjRestart Status is the new graceful restart state of the adjacency.
Effect	No effect.
Recovery	No recovery is necessary.

29.4 tmnxIsisAreaMismatch

Table 547: tmnxIsisAreaMismatch properties

Property name	Value
Application name	ISIS
Event ID	2040
Event name	tmnxIsisAreaMismatch
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.12
Default severity	warning
Message format string	Area mismatch on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, fragment: *$vRtrIsisPDUFragmentString$*, LSP size: *$tmnxIsisNotifLSPSize$*
Cause	The tmnxIsisAreaMismatch notification is sent when we receive a Hello PDU from an IS which does not share any area address. This notification includes the header of the packet, which may help a network manager identify the source of the confusion. This should be an edge-triggered notification. We should not send a second notification about PDUs received from what seem to be the same source. This decision is up to the agent to make, and may be based on the circuit or on some MAC level information.
Effect	No effect.
Recovery	No recovery is necessary.

29.5 tmnxIsisAuthFail

Table 548: tmnxIsisAuthFail properties

Property name	Value
Application name	ISIS
Event ID	2038
Event name	tmnxIsisAuthFail
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.10
Default severity	warning
Message format string	Authentication failure on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, fragment: *$vRtrIsisPDUFragmentString$*

Property name	Value
Cause	The tmnxIsisAuthFail notification is sent when we receive a PDU with incorrect authentication information field. This notification includes the header of the packet, which may help a network manager identify the source of the confusion. This should be an edge-triggered notification. We should not send a second notification about PDUs received from what seem to be the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.6 tmnxIsisAutTypeFail

Table 549: tmnxIsisAutTypeFail properties

Property name	Value
Application name	ISIS
Event ID	2037
Event name	tmnxIsisAutTypeFail
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.9
Default severity	warning
Message format string	Authentication type failure on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, fragment: *$vRtrIsisPDUFragmentString$*
Cause	The tmnxIsisAutTypeFail notification is sent when we receive a PDU with the wrong authentication type field. This notification includes the header of the packet, which may help a network manager identify the source of the confusion. This should be an edge-triggered notification. We should not send a second notification about PDUs received from what seem to be the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.7 tmnxIsisCircIdExhausted

Table 550: tmnxIsisCircIdExhausted properties

Property name	Value
Application name	ISIS
Event ID	2046
Event name	tmnxIsisCircIdExhausted
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.18
Default severity	warning
Message format string	Circuit-id space exhausted for level *$tmnxIsisNotifSystemLevel$* - interface: *$vRtrIfIndex$*
Cause	The tmnxIsisCircIdExhausted notification is sent when the specific ISIS level cannot be started on a LAN interface as a unique circid could not be assigned due to the exhaustion of the circid space. This could happen only on the broadcast interfaces.
Effect	In such a case the interface is marked operationally down.
Recovery	When an operationally up interface is deleted, the circid can be reused by any interface which is waiting to receive a unique circid.

29.8 tmnxIsisCorruptedLSPDetected

Table 551: tmnxIsisCorruptedLSPDetected properties

Property name	Value
Application name	ISIS
Event ID	2031
Event name	tmnxIsisCorruptedLSPDetected
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.3
Default severity	warning
Message format string	Corrupted LSP detected on level: *$tmnxIsisNotifSystemLevel$*, with LSP-id: *$vRtrIsisTrapLSPIDString$*.
Cause	The tmnxIsisCorruptedLSPDetected notification is generated when we find that and LSP that was stored in memory has become corrupted. We forward an LSP ID. We may have independent knowledge of the

Property name	Value
	ID, but in some implementations there is a chance that the ID itself will be corrupted.
Effect	LSP is dropped.
Recovery	No recovery is necessary.

29.9 tmnxIsisDatabaseOverload

Table 552: tmnxIsisDatabaseOverload properties

Property name	Value
Application name	ISIS
Event ID	2029
Event name	tmnxIsisDatabaseOverload
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.1
Default severity	warning
Message format string	Overload (event *$tmnxIsisLevelOverloadStatus$*, system level: *$tmnxIsisNotifSystemLevel$*) - Level1State: *$isisSysL1State$*, Level2State: *$isisSysL2State$ $tmnxIsisNotifyDescription$*
Cause	The tmnxIsisDatabaseOverload notification is generated when the system enters or leaves the Overload state.
Effect	Database is overloaded.
Recovery	No recovery is necessary.

29.10 tmnxIsisExportLimitReached

Table 553: tmnxIsisExportLimitReached properties

Property name	Value
Application name	ISIS
Event ID	2050
Event name	tmnxIsisExportLimitReached
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.22

Property name	Value
Default severity	major
Message format string	ISIS level *$tmnxIsisNotifSystemLevel$* has reached the export-limit *$tmnxIsisExportLimit$*, additional routes will not be exported into this ISIS level
Cause	The tmnxIsisExportLimitReached notification is sent when the total number of exported routes for the level is equal to the configured limit for exported routes, tmnxIsisExportLimit.
Effect	Additional routes would not be exported into this ISIS level from the route table.
Recovery	Change ISIS export policy.

29.11 tmnxIsisExportLimitWarning

Table 554: tmnxIsisExportLimitWarning properties

Property name	Value
Application name	ISIS
Event ID	2051
Event name	tmnxIsisExportLimitWarning
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.23
Default severity	warning
Message format string	ISIS level *$tmnxIsisNotifSystemLevel$* has reached *$tmnxIsisExport LimitLogPercent$* percent of the export limit *$tmnxIsisExportLimit$*
Cause	The tmnxIsisExportLimitWarning notification is sent when the total number of exported routes or the level is equal to the configured percent, tmnxIsisExportLimitLogPercent of the export limit, tmnxIsis ExportLimit. Additional routes will continue to be exported into this ISIS level from the route table till the export limit is reached.
Effect	No effect.
Recovery	No recovery is necessary.

29.12 tmnxIsisFailureDisabled

Table 555: tmnxIsisFailureDisabled properties

Property name	Value
Application name	ISIS
Event ID	2056
Event name	tmnxIsisFailureDisabled
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.28
Default severity	minor
Message format string	ISIS disabled. Reason : *$tmnxIsisFailureReasonCode$*
Cause	A tmnxIsisFailureDisabled notification is generated when ISIS is operationally brought down. Reason for the failure is indicated by tmnx IsisFailureReasonCode.
Effect	ISIS is now operationally down.
Recovery	ISIS will auto restart.

29.13 tmnxIsisIDLenMismatch

Table 556: tmnxIsisIDLenMismatch properties

Property name	Value
Application name	ISIS
Event ID	2033
Event name	tmnxIsisIDLenMismatch
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.5
Default severity	warning
Message format string	ISIS-id length mismatch - field length: *$tmnxIsisNotifFieldLen$*, interface: *$vRtrIfIndex$*, on fragment: *$vRtrIsisPDUFragmentString$*
Cause	The tmnxIsisIDLenMismatch notification is sent when we receive a PDU with a different value of the System ID Length. This notification includes the index to identify the circuit where we saw the PDU and the header of the PDU which may help a network manager identify the source of the confusion. This should be an edge-triggered notification. We should not send a second notification about PDUs received from what seem to be the same source. This decision is up to the agent

Property name	Value
	to make, and may be based on the circuit or on some MAC level information.
Effect	No effect.
Recovery	No recovery is necessary.

29.14 tmnxIsisLdpSyncExit

Table 557: tmnxIsisLdpSyncExit properties

Property name	Value
Application name	ISIS
Event ID	2049
Event name	tmnxIsisLdpSyncExit
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.21
Default severity	warning
Message format string	IGP-LDP synchronization has stopped for interface *$vRtrIfIndex$* because Exit State *$tmnxIsisIfLdpSyncTimerState$*
Cause	The tmnxIsisLdpSyncExit notification is sent when IGP-LDP synchronization has stopped. The cause of this event is indicated by tmnxIsisIfLdpSyncTimerState, one of them being expiry of vRtrIfLdp SyncTimer.
Effect	The IGP link metric is restored to normal levels.
Recovery	No recovery is necessary.

29.15 tmnxIsisLdpSyncTimerStarted

Table 558: tmnxIsisLdpSyncTimerStarted properties

Property name	Value
Application name	ISIS
Event ID	2048
Event name	tmnxIsisLdpSyncTimerStarted

Property name	Value
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.20
Default severity	warning
Message format string	IGP-LDP synchronization timer has started for interface *$vRtrIfIndex$*.
Cause	The tmnxIsisLdpSyncTimerStarted notification is sent when the vRtr IfLdpSyncTimer is started. The timer is started from the time the LDP session to the neighbor is up over the interface.
Effect	This allows for the label FEC bindings to be exchanged.
Recovery	No recovery is necessary.

29.16 tmnxIsisLSPPurge

Table 559: tmnxIsisLSPPurge properties

Property name	Value
Application name	ISIS
Event ID	2060
Event name	tmnxIsisLSPPurge
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.32
Default severity	warning
Message format string	Possible messages: • LSP Purge - interface: *$vRtrIfIndex$*, on level: *$tmnxIsisNotifSystemLevel$*, LSP: *$vRtrIsisTrapLSPIDString$*, POI SysId: *$tmnxIsisNotifPurgeOriginatorString$* - *$tmnxIsisNotifAdditionalInfo$* • LSP Purge - interface: *$vRtrIfIndex$*, on level: *$tmnxIsisNotifSystemLevel$*, LSP: *$vRtrIsisTrapLSPIDString$*, POI sysId: *$tmnxIsisNotifPurgeOriginatorString$*, rcvd sysId: *$tmnxIsisNotifPurgeSourceString$* - *$tmnxIsisNotifAdditionalInfo$*
Cause	The tmnxIsisLSPPurge notification is sent when a LSP is purged. This notification includes the system ID of the originator, or the upstream source of the purge, which may help a network manager to locate the origin of the purge and thus the cause of the purge.
Effect	No effect.
Recovery	No recovery is necessary.

29.17 tmnxIsisLSPTooLargeToPropagate

Table 560: tmnxIsisLSPTooLargeToPropagate properties

Property name	Value
Application name	ISIS
Event ID	2042
Event name	tmnxIsisLSPTooLargeToPropagate
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.14
Default severity	warning
Message format string	LSP too large to propagate - LSP size: *$tmnxIsisNotifLSPSize$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, LSP-id: *$vRtrIsisTrapLSPIDString$*
Cause	The tmnxIsisLSPTooLargeToPropagate notification is sent when we attempt to propagate an LSP which is larger than the dataLinkBlock Size for a circuit. This should be an edge-triggered notification. We should not send a second notification about PDUs received from the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.18 tmnxIsisManualAddressDrops

Table 561: tmnxIsisManualAddressDrops properties

Property name	Value
Application name	ISIS
Event ID	2030
Event name	tmnxIsisManualAddressDrops
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.2
Default severity	warning
Message format string	Configured manual area address *$isisManAreaAddrString$* being ignored when computing routes

Property name	Value
Cause	This notification is generated when one of the manual area addresses assigned to this system is ignored when computing routes. The object isisManAreaAddrExistState describes the area that has been dropped. This notification is edge triggered, and should not be regenerated until an address that was used in the previous computation has been dropped.
Effect	Assigned manual area address is ignored for computing routes.
Recovery	No recovery is necessary.

29.19 tmnxIsisMaxAreaAddrsMismatch

Table 562: tmnxIsisMaxAreaAddrsMismatch properties

Property name	Value
Application name	ISIS
Event ID	2034
Event name	tmnxIsisMaxAreaAddrsMismatch
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.6
Default severity	warning
Message format string	Max area addresses mismatch - max area addresses: *$tmnxIsisNotifMaxAreaAddress$*, interface: *$vRtrIfIndex$*, on fragment: *$vRtrIsisPDUFragmentString$*
Cause	The tmnxIsisMaxAreaAddrsMismatch notification is sent when we receive a PDU with a different value of the Maximum Area Addresses. This notification includes the header of the packet, which may help a network manager identify the source of the confusion. This should be an edge-triggered notification. We should not send a second notification about PDUs received from what seem to be the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.20 tmnxIsisMaxSeqExceedAttempt

Table 563: tmnxIsisMaxSeqExceedAttempt properties

Property name	Value
Application name	ISIS
Event ID	2032
Event name	tmnxIsisMaxSeqExceedAttempt
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.4
Default severity	warning
Message format string	Attempt to exceed the maximum sequence on level: *$tmnxIsisNotifSystemLevel$*, with LSP-id: *$vRtrIsisTrapLSPIDString$*.
Cause	The tmnxIsisMaxSeqExceedAttempt notification is generated when the sequence number on an LSP wraps the 32 bit sequence counter, we purge and wait to re-announce this information. Since these should not be generated rapidly, we generate an event each time this happens. While the first 6 bytes of the LSPID are ours, the other two contain useful information.
Effect	No effect.
Recovery	No recovery is necessary.

29.21 tmnxIsisOrigLSPBufSizeMismatch

Table 564: tmnxIsisOrigLSPBufSizeMismatch properties

Property name	Value
Application name	ISIS
Event ID	2043
Event name	tmnxIsisOrigLSPBufSizeMismatch
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.15
Default severity	warning
Message format string	Originating LSP buffer size mismatch - LSP size: *$tmnxIsisNotifOriginatingBuffSize$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, LSP-id: *$vRtrIsisTrapLSPIDString$*
Cause	The tmnxIsisOrigLSPBufSizeMismatch notification is sent when a Level 1 LSP or Level 2 LSP is received which is larger than the local value for

Property name	Value
	isisSysOrigL1LSPBuffSize or isisSysOrigL2LSPBuffSize respectively, or when a Level 1 LSP or Level2 LSP is received containing the originatingLSPBufferSize option and the value in the PDU option field does not match the local value for isisSysOrigL1LSPBuffSize or isis SysOrigL2LSPBuffSize respectively. We pass up the size from the option field or the size of the LSP that exceeds our configuration. This should be an edge-triggered notification. We should not send a second notification about PDUs received from the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.22 tmnxIsisOwnLSPPurge

Table 565: tmnxIsisOwnLSPPurge properties

Property name	Value
Application name	ISIS
Event ID	2035
Event name	tmnxIsisOwnLSPPurge
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.7
Default severity	warning
Message format string	Own LSP Purge - interface: *$vRtrIfIndex$*, on level: *$tmnxIsisNotif SystemLevel$*, LSP: *$vRtrIsisTrapLSPIDString$*
Cause	The tmnxIsisOwnLSPPurge notification is sent when we receive a PDU with our SystemID and zero age. This notification includes the circuit Index if available, which may help a network manager identify the source of the confusion.
Effect	No effect.
Recovery	No recovery is necessary.

29.23 tmnxIsisPfxLimitOverloadWarning

Table 566: tmnxIsisPfxLimitOverloadWarning properties

Property name	Value
Application name	ISIS
Event ID	2061
Event name	tmnxIsisPfxLimitOverloadWarning
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.33
Default severity	warning
Message format string	Overload warning *$tmnxIsisNotifAdditionalInfo$*
Cause	The tmnxIsisPfxLimitOverloadWarning notification is sent when the number of prefixes in the system reaches the tmnxIsisPrefixLimit Threshold or the tmnxIsisPrefixLimit.
Effect	When tmnxIsisPrefixLimit is not yet reached, but the tmnxIsisPrefixLimit Threshold is reached there is no direct effect; but when the number of prefixes grows the system migth go in overload. When the tmnxIsis PrefixLimit is reached and the object tmnxIsisPrefixLimitLogOnly is false, IS-IS will be in overload. There is no direct effect when the object tmnxIsisPrefixLimitLogOnly is true.
Recovery	Increase the IS-IS prefix limit.

29.24 tmnxIsisProtoSuppMismatch

Table 567: tmnxIsisProtoSuppMismatch properties

Property name	Value
Application name	ISIS
Event ID	2044
Event name	tmnxIsisProtoSuppMismatch
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.16
Default severity	warning
Message format string	Supported protocol mismatch - supported protocol: *$tmnxIsisNotif ProtocolsSupported$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsis NotifSystemLevel$*, LSP-id: *$vRtrIsisTrapLSPIDString$*

Property name	Value
Cause	The tmnxIsisProtoSuppMismatch notification is sent when a non-pseudonode segment 0 LSP is received that has no matching protocols supported. This may be because the system does not generate the field, or because there are no common elements. The list of protocols supported should be included in the notification: it may be empty if the TLV is not supported, or if the TLV is empty. This should be an edge-triggered notification. We should not send a second notification about PDUs received from the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.25 tmnxIsisRejectedAdjacency

Table 568: tmnxIsisRejectedAdjacency properties

Property name	Value
Application name	ISIS
Event ID	2041
Event name	tmnxIsisRejectedAdjacency
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.13
Default severity	warning
Message format string	Rejected adjacency on interface: *$vRtrIfIndex$*, for level:*$tmnxIsisNotifSystemLevel$*
Cause	The tmnxIsisRejectedAdjacency notification is sent when we receive a Hello PDU from an IS, but do not establish an adjacency due to a lack of resources. This should be an edge-triggered notification. We should not send a second notification about PDUs received from the same source.
Effect	No effect.
Recovery	No recovery is necessary.

29.26 tmnxIsisRejectedAdjacencySid

Table 569: tmnxIsisRejectedAdjacencySid properties

Property name	Value
Application name	ISIS
Event ID	2059
Event name	tmnxIsisRejectedAdjacencySid
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.31
Default severity	warning
Message format string	Failed SID adjacency on interface: *$vRtrIfIndex$*, for level:*$tmnxIsisNotifSystemLevel$*, description: *$tmnxIsisNotifyDescription$*
Cause	The tmnxIsisRejectedAdjacencySid notification is sent when we do not establish an adjacency SID due to a lack of resources. This should be an edge-triggered notification. We should not send a second notification about adjacency SID allocation failure for the same adjacency.
Effect	No effect.
Recovery	When an operationally up interface is deleted, the ADJ-SID can be reused by any interface which is waiting to receive an ADJ-SID.

29.27 tmnxIsisRoutesExpLmtDropped

Table 570: tmnxIsisRoutesExpLmtDropped properties

Property name	Value
Application name	ISIS
Event ID	2052
Event name	tmnxIsisRoutesExpLmtDropped
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.24
Default severity	warning
Message format string	The number of redistributed routes into ISIS level *$tmnxIsisNotifSystemLevel$* has dropped below the export limit *$tmnxIsisExportLimit$*

Property name	Value
Cause	The tmnxIsisRoutesExpLmtDropped notification is sent when the total number of exported routes from the route table to this ISIS level drops below the configured export limit, tmnxIsisExportLimit.
Effect	No effect.
Recovery	No recovery is necessary.

29.28 tmnxIsisSequenceNumberSkip

Table 571: tmnxIsisSequenceNumberSkip properties

Property name	Value
Application name	ISIS
Event ID	2036
Event name	tmnxIsisSequenceNumberSkip
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.8
Default severity	warning
Message format string	Sequence number skipped for LSP: *$vRtrIsisTrapLSPIDString$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*
Cause	The tmnxIsisSequenceNumberSkip notification is sent when we need to increase the sequence number by more than one. When we receive an LSP with out System ID and different contents, we may need to reissue the LSP with a higher sequence number. If two Intermediate Systems are configured with the same System ID, this notification will fire.
Effect	No effect.
Recovery	No recovery is necessary.

29.29 tmnxIsisSidError

Table 572: tmnxIsisSidError properties

Property name	Value
Application name	ISIS
Event ID	2057

Property name	Value
Event name	tmnxIsisSidError
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.29
Default severity	minor
Message format string	*$tmnxIsisNotifyDescription$* SID: *$tmnxIsisPrefixSidValue$*, level:*$tmnxIsisPrefixSidLevel$*, mtid: *$tmnxIsisRouteMtId$*, type:*$tmnxIsisPrefixSidType$*, flags: *$tmnxIsisPrefixSidFlags$*
Cause	This notification is generated when ISIS receives an IOM or CPM failure (system exhausted ILM, NHLFE, duplicate SID) while resolving and programming a received prefix SID.
Effect	The Segment Routing tunnel corresponding to this SID will not be programmed.
Recovery	In case of system exhaustion, the IGP instance goes into overload. The operator must manually clear the IGP overload condition after freeing resources. IGP will attempt to program at the next SPF all tunnels which previously failed the programming operation

29.30 tmnxIsisSidNotInLabelRange

Table 573: tmnxIsisSidNotInLabelRange properties

Property name	Value
Application name	ISIS
Event ID	2058
Event name	tmnxIsisSidNotInLabelRange
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.30
Default severity	minor
Message format string	SID not in range of router: *$tmnxIsisNotifPfxSidSysIDString$*, SID:*$tmnxIsisPrefixSidValue$*, startLabel: *$tmnxIsisNotifPfxSidRangeStartLbl$*, maxIdx:*$tmnxIsisNotifPfxSidRangeMaxIdx$* level: *$tmnxIsisPrefixSidLevel$*, mtid:*$tmnxIsisRouteMtId$*, type: *$tmnxIsisPrefixSidType$*, flags:*$tmnxIsisPrefixSidFlags$*
Cause	This notification is generated when ISIS receives a SID which is not within the label range of the nhop router.
Effect	The Segment Routing tunnel corresponding to this SID will not be programmed.

Property name	Value
Recovery	Increase the label range or change the SID index to be within the current label range.

29.31 tmnxIsisSpbEctFidCfgChg

Table 574: tmnxIsisSpbEctFidCfgChg properties

Property name	Value
Application name	ISIS
Event ID	2055
Event name	tmnxIsisSpbEctFidCfgChg
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.27
Default severity	warning
Message format string	SPB ect-algorithm changed to *$vRtrSpbEctFidAlgorithm$* for FID range *$tmnxIsisSpbEctFidStart$- $tmnxIsisSpbEctFidEnd$* under *$vRtrIsis Level$*
Cause	A tmnxIsisSpbEctFidCfgChg notification is sent when a configuration change is made to vRtrSpbEctFidTable affecting forwarding database identifiers in the range from tmnxIsisSpbEctFidStart to tmnxIsisSpbEct FidEnd.
Effect	There are changes in the vRtrSpbEctFidTable which may be out-of-sync with management application.
Recovery	Management application may need to synchronize with changes in the vRtrSpbEctFidTable.

29.32 tmnxIsisSpbNbrMultAdjExists

Table 575: tmnxIsisSpbNbrMultAdjExists properties

Property name	Value
Application name	ISIS
Event ID	2053
Event name	tmnxIsisSpbNbrMultAdjExists
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.25

Property name	Value
Default severity	warning
Message format string	SPB multiple adjacency exists for neighbor *$vRtrIsisNbrSysIdString$* at system level *$tmnxIsisNotifSystemLevel$*
Cause	A tmnxIsisSpbNbrMultAdjExists notification is sent when IS-IS SPB instance detects a neighbor to which it already has a direct adjacency on another interface.
Effect	During SPF IS-IS SPB instance will have incorrect neighbor information and hence path computations will be incorrect.
Recovery	Check number of links to neighbor to make sure there is only one link.

29.33 tmnxIsisSpbNbrMultAdjExistsClear

Table 576: tmnxIsisSpbNbrMultAdjExistsClear properties

Property name	Value
Application name	ISIS
Event ID	2054
Event name	tmnxIsisSpbNbrMultAdjExistsClear
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.26
Default severity	warning
Message format string	SPB multiple adjacency cleared for neighbor *$vRtrIsisNbrSysIdString$* at system level *$tmnxIsisNotifSystemLevel$*
Cause	A tmnxIsisSpbNbrMultAdjExistsClear notification is sent when an IS-IS SPB instance clears the condition raised by tmnxIsisSpbNbrMultAdj Exists notification.
Effect	During SPF IS-IS SPB instance will have correct neighbor information and hence path computations will be correct.
Recovery	None required.

29.34 tmnxIsisSrgbBadLabelRange

Table 577: tmnxIsisSrgbBadLabelRange properties

Property name	Value
Application name	ISIS
Event ID	2063
Event name	tmnxIsisSrgbBadLabelRange
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.35
Default severity	warning
Message format string	Bad SRGB label range for advertising router: *$tmnxIsisNotifSrgbAdvRtrSysIDString$*, startLabel:*$tmnxIsisNotifSrgbRangeStartLbl$*, max Idx: *$tmnxIsisNotifSrgbRangeMaxIdx$*, level:*$tmnxIsisNotifSrgbLevel$*, mtid: *$tmnxIsisNotifSrgbMtId$ $tmnxIsisNotifAdditionalInfo$*
Cause	The tmnxIsisSrgbBadLabelRange notification is sent when ISIS receives a bad SRGB label range from a router (for example, overlapping with another label range).
Effect	The configured Segment Routing tunnels will be wrong.
Recovery	Change the label range to recover.

29.35 tmnxIsisVersionSkew

Table 578: tmnxIsisVersionSkew properties

Property name	Value
Application name	ISIS
Event ID	2039
Event name	tmnxIsisVersionSkew
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.11
Default severity	warning
Message format string	Protocol version skew - *$tmnxIsisNotifProtocolVersion$* on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, fragment: *$vRtrIsisPDUFragmentString$*
Cause	The tmnxIsisVersionSkew notification is sent when we receive a Hello PDU from an IS running a different version of the protocol. This notification includes the header of the packet, which may help

Property name	Value
	a network manager identify the source of the confusion. This should be an edge-triggered notification. We should not send a second notification about PDUs received from what seem to be the same source. This decision is up to the agent to make, and may be based on the circuit or on some MAC level information.
Effect	No effect.
Recovery	No recovery is necessary.

29.36 vRtrIsisSpbNbrMultAdjExists

Table 579: vRtrIsisSpbNbrMultAdjExists properties

Property name	Value
Application name	ISIS
Event ID	2025
Event name	vRtrIsisSpbNbrMultAdjExists
SNMP notification prefix and OID	TIMETRA-ISIS-MIB.vRtrIsisNotifications.25
Default severity	warning
Message format string	SPB multiple adjacency exists for neighbor *$vRtrIsisNbrSysIdString$* at system level *$vRtrIsisSystemLevel$*
Cause	A vRtrIsisSpbNbrMultAdjExists notification is sent when IS-IS SPB instance detects a neighbor to which it already has a direct connection to it on another interface.
Effect	During SPF IS-IS SPB instance will have incorrect neighbor information and hence the computation will be incorrect.
Recovery	Check number of links to neighbor to make sure there is only one link.

29.37 vRtrIsisSpbNbrMultAdjExistsClear

Table 580: vRtrIsisSpbNbrMultAdjExistsClear properties

Property name	Value
Application name	ISIS
Event ID	2026

Property name	Value
Event name	vRtrIsisSpbNbrMultAdjExistsClear
SNMP notification prefix and OID	TIMETRA-ISIS-MIB.vRtrIsisNotifications.26
Default severity	warning
Message format string	SPB multiple adjacency cleared for neighbor *$vRtrIsisNbrSysIdString$* at system level *$vRtrIsisSystemLevel$*
Cause	A vRtrIsisSpbNbrMultAdjExistsClear notification is sent when an IS-IS SPB instance clears the condition raised by vRtrIsisSpbNbrMultAdj Exists notification.
Effect	During SPF IS-IS SPB instance will have correct neighbor information and hence the computation will be correct.
Recovery	None required.

29.38 vRtrSpbEctFidCfgChg

Table 581: vRtrSpbEctFidCfgChg properties

Property name	Value
Application name	ISIS
Event ID	2027
Event name	vRtrSpbEctFidCfgChg
SNMP notification prefix and OID	TIMETRA-ISIS-MIB.vRtrIsisNotifications.27
Default severity	warning
Message format string	SPB ect-algorithm changed to *$vRtrSpbEctFidAlgorithm$* for FID range *$vRtrSpbEctFidStart$- $vRtrSpbEctFidEnd$* under *$vRtrIsisLevel$*
Cause	A vRtrSpbEctFidCfgChg notification is sent when a configuration change is made to vRtrSpbEctFidTable affecting forwarding database identifiers in the range from vRtrSpbEctFidStart to vRtrSpbEctFidEnd.
Effect	There are changes in the vRtrSpbEctFidTable which may be out-of-sync with management application.
Recovery	Management application may need to synchronize with changes in the vRtrSpbEctFidTable.

30 L2TP

30.1 tmnxL2tpApFailure

Table 582: tmnxL2tpApFailure properties

Property name	Value
Application name	L2TP
Event ID	2011
Event name	tmnxL2tpApFailure
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.11
Default severity	warning
Message format string	RADIUS accounting policy tmnxSubAcctPlcyName failure - *$tmnxL2tpNotifyDescription$*.
Cause	The tmnxL2tpApFailure notification is generated when a RADIUS accounting request was not sent out successfully to any of the RADIUS servers in the indicated accounting policy.
Effect	N/A
Recovery	N/A

30.2 tmnxL2tpIsaMdaVRtrStateChange

Table 583: tmnxL2tpIsaMdaVRtrStateChange properties

Property name	Value
Application name	L2TP
Event ID	2002
Event name	tmnxL2tpIsaMdaVRtrStateChange
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.2
Default severity	minor

Property name	Value
Message format string	The operational state changed to *$tmnxL2tpIsaMdaVRtrOperState$*. *$tmnxL2tpNotifyDescription$*.
Cause	The tmnxL2tpIsaMdaVRtrStateChange notification is sent when the operational state of an L2TP ISA MDA with respect to a Virtual Router changes.
Effect	N/A
Recovery	N/A

30.3 tmnxL2tpLnsPppNcpFailure

Table 584: tmnxL2tpLnsPppNcpFailure properties

Property name	Value
Application name	L2TP
Event ID	2010
Event name	tmnxL2tpLnsPppNcpFailure
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.10
Default severity	warning
Message format string	PPP *$tmnxL2tpPppNcpFailureProtocol$* phase failure for user *$tmnxL2tpLnsSePppPppUserName$* interface *$vRtrIfName$* service *$tmnxL2tpLnsSePppSvcId$* - *$tmnxL2tpNotifyDescription$*
Cause	The tmnxL2tpLnsPppNcpFailure notification indicates that there is an NCP phase setup problem.
Effect	N/A
Recovery	N/A

30.4 tmnxL2tpLnsSePppSessionFailure

Table 585: tmnxL2tpLnsSePppSessionFailure properties

Property name	Value
Application name	L2TP
Event ID	2003

Property name	Value
Event name	tmnxL2tpLnsSePppSessionFailure
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.3
Default severity	warning
Message format string	Failed to create session for user *$tmnxL2tpLnsSePppPppUserName $* interface *$vRtrIfName$* service *$tmnxL2tpLnsSePppSvcId$* - *$tmnxL2tpNotifyDescription$*
Cause	The tmnxL2tpLnsSePppSessionFailure notification is sent when the system could not create a new session in the tmnxL2tpLnsSePppTable.
Effect	N/A
Recovery	N/A

30.5 tmnxL2tpPeerUnreachable

Table 586: tmnxL2tpPeerUnreachable properties

Property name	Value
Application name	L2TP
Event ID	2001
Event name	tmnxL2tpPeerUnreachable
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.1
Default severity	warning
Message format string	The unreachability of L2TP peer *$tmnxL2tpTuStatusPeerAddr$* (port *$tmnxL2tpTuStatusRemoteUdpPort$*) changed to *$tmnxL2tpPeerStat Unreachable$*. *$tmnxL2tpNotifyDescription$*.
Cause	The tmnxL2tpPeerUnreachable notification is generated when the peer becomes unreachable, and then becomes reachable again. The cause may be specified in the tmnxL2tpNotifyDescription.
Effect	N/A
Recovery	N/A

30.6 tmnxL2tpTunnelBlacklisted

Table 587: tmnxL2tpTunnelBlacklisted properties

Property name	Value
Application name	L2TP
Event ID	2006
Event name	tmnxL2tpTunnelBlacklisted
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.12
Default severity	minor
Message format string	The unreachability of L2TP tunnel $tmnxL2tpTuStatusId in vRtr $vRtr Id changed to $tmnxL2tpTuStatusSelBlacklstState. *$tmnxL2tpNotify Description$*.
Cause	The tmnxL2tpTunnelBlacklisted notification is sent when a L2TP tunnel is added to or removed from the tunnel-selection-blacklist.
Effect	N/A
Recovery	N/A

30.7 tmnxL2tpTunnelSelBlacklistFull

Table 588: tmnxL2tpTunnelSelBlacklistFull properties

Property name	Value
Application name	L2TP
Event ID	2007
Event name	tmnxL2tpTunnelSelBlacklistFull
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.13
Default severity	minor
Message format string	The full-state L2TP tunnel-selection-blacklist of vRtr $vRtrId changed. There are now $tmnxL2tpStatCurrSelBlacklstLen entries in the blacklist, out of a maximum of $tmnxL2tpXtTuSelBlacklistLength. *$tmnxL2tpNotifyDescription$*.
Cause	The tmnxL2tpTunnelBlacklistFull notification is sent when the number of tunnels and peers in the tunnel-selection-blacklist reaches the limit

Property name	Value
	configured in tmnxL2tpXtTuSelBlacklistLength, or when the limit is no longer reached.
Effect	N/A
Recovery	N/A

31 LAG

31.1 DynamicCostOff

Table 589: DynamicCostOff properties

Property name	Value
Application name	LAG
Event ID	2002
Event name	DynamicCostOff
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.2
Default severity	warning
Message format string	LAG *$tLagIndex$* exited dynamic-cost mode
Cause	A sufficient number of ports in the LAG repaired, so the remaining number of operational ports in the LAG was greater than the port threshold.
Effect	The LAG exits dynamic-cost mode; OSPF and other services on the LAG change their cost.
Recovery	No recovery is necessary.

31.2 DynamicCostOn

Table 590: DynamicCostOn properties

Property name	Value
Application name	LAG
Event ID	2001
Event name	DynamicCostOn
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.1
Default severity	warning
Message format string	LAG *$tLagIndex$* entered dynamic-cost mode

Property name	Value
Cause	A sufficient number of ports in the LAG failed, so the remaining number of operational ports in the LAG was less than or equal to the port threshold.
Effect	The LAG enters dynamic-cost mode; OSPF and other services on the LAG change their cost.
Recovery	Either repair enough physical ports so that the number of operational ports in the LAG is greater than or equal to the port threshold, change the port threshold, or change the port threshold action from dynamic-cost to down.

31.3 LagPortAddFailed

Table 591: LagPortAddFailed properties

Property name	Value
Application name	LAG
Event ID	2003
Event name	LagPortAddFailed
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.3
Default severity	warning
Message format string	Could not add port *$tmnxPortPortID$* to LAG *$tLagIndex$* because *$t LagNotifyPortAddFailReason$*
Cause	The tLagPortAddFailed notification is generated when a port failed to be added to the lag.
Effect	Dependent upon the value of tLagNotifyPortAddFailReason.
Recovery	Dependent upon the value of tLagNotifyPortAddFailReason.

31.4 LagPortAddFailureCleared

Table 592: LagPortAddFailureCleared properties

Property name	Value
Application name	LAG
Event ID	2005

Property name	Value
Event name	LagPortAddFailureCleared
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.5
Default severity	warning
Message format string	Failure to add port *$tmnxPortPortID$* to LAG *$tLagIndex$* is resolved - *$tLagNotifyPortAddFailReason$*
Cause	The failure reported by notification tLagPortAddFailed has been resolved.
Effect	N/A
Recovery	N/A

31.5 LagStateEvent

Table 593: LagStateEvent properties

Property name	Value
Application name	LAG
Event ID	2006
Event name	LagStateEvent
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.6
Default severity	warning
Message format string	LAG *$tLagIndex$* : *$tLagNotifyAdditionalInfo$*
Cause	The cause described in this event may influence the LAG state.
Effect	The state of the LAG may change.
Recovery	No action needed.

31.6 LagSubGroupSelected

Table 594: LagSubGroupSelected properties

Property name	Value
Application name	LAG

Property name	Value
Event ID	2004
Event name	LagSubGroupSelected
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.4
Default severity	warning
Message format string	*$tLagNotifySubGroupSelected$*
Cause	The tLagSubGroupSelected notification is generated when the selection algorithm selects a different sub-group.
Effect	No effect.
Recovery	No recovery is necessary.

31.7 tLagMemberStateEvent

Table 595: tLagMemberStateEvent properties

Property name	Value
Application name	LAG
Event ID	2007
Event name	tLagMemberStateEvent
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.7
Default severity	warning
Message format string	LAG *$tLagIndex$* : *$tLagNotifyAdditionalInfo$*
Cause	The cause described in this event may influence the LAG state.
Effect	The state of the LAG may change.
Recovery	No action needed.

31.8 tmnxLagBfdMemStateChanged

Table 596: tmnxLagBfdMemStateChanged properties

Property name	Value
Application name	LAG
Event ID	2008
Event name	tmnxLagBfdMemStateChanged
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.8
Default severity	minor
Message format string	LAG *$tLagIndex$* member *$tmnxPortPortID$* BFD state changed to *$tmnxLagBfdMemState$* - *$tLagNotifyAdditionalInfo$*
Cause	The tmnxLagBfdMemStateChanged notification is sent when the value of an instance of the object tmnxLagBfdMemState changes. The cause is explained in the tLagNotifyAdditionalInfo.
Effect	While the value of the object tmnxLagBfdMemState is equal to - 'idle', 'failed', 'waitingFwd', 'up': the port is forwarding traffic; - 'waiting', 'down': the port is not forwarding traffic.
Recovery	The recovery action will depend on the actual cause as specified in the tLagNotifyAdditionalInfo.

32 LDAP

32.1 tmnxLdapOperStateChange

Table 597: tmnxLdapOperStateChange properties

Property name	Value
Application name	LDAP
Event ID	2001
Event name	tmnxLdapOperStateChange
SNMP notification prefix and OID	TIMETRA-LDAP-MIB.tmnxLdapNotifications.1
Default severity	major
Message format string	Operational state of the LDAP protocol has changed to *$tmnxLdap OperState$*
Cause	[CAUSE]The tmnxLdapOperStateChange notification is generated when the tmnxLdapOperState has transitioned either from 'out OfService' to 'inService' or from 'inService' to 'outOfService' state. [EFFECT]If tmnxLdapOperState has transitioned to 'outOfService' state then the LDAP protocol is not available for use. If tmnxLdapOper State has transitioned to 'inService' state then the LDAP protocol is available for use. [RECOVERY]If the new state corresponds to the value of tmnxLdapAdminState, then this is desirable behavior and no recovery is needed. If the new state of the tmnxLdapOperState object is 'outOfService' while the value of the object tmnxLdapAdminState is 'inService', make sure that the value of tmnxLdapServerOperState of at least one LDAP server connection is 'inService'.
Effect	N/A
Recovery	N/A

32.2 tmnxLdapServerOperStateChange

Table 598: tmnxLdapServerOperStateChange properties

Property name	Value
Application name	LDAP

Property name	Value
Event ID	2002
Event name	tmnxLdapServerOperStateChange
SNMP notification prefix and OID	TIMETRA-LDAP-MIB.tmnxLdapNotifications.2
Default severity	minor
Message format string	Operational state of the connection to the LDAP server ' *$tmnxLdapServerName$*' (ID: *$tmnxLdapServerIndex$*) (*$tmnxLdapServerInetAddress$*: *$tmnxLdapServerPort$*) has changed to *$tmnxLdapServerOperState$*
Cause	[CAUSE]The tmnxLdapServerOperStateChange notification is generated when the tmnxLdapServerOperState has transitioned either from 'outOfService' to 'inService' or from 'inService' to 'outOfService' state. [EFFECT]If tmnxLdapServerOperState has transitioned to 'out OfService' state then the particular LDAP server connection is not available for use. If tmnxLdapServerOperState has transitioned to 'in Service' state then the particular LDAP server is available for use. [RECOVERY]If the new state corresponds to the tmnxLdapServer AdminState, then this is the desirable behavior and no recovery is needed. If the new state of the tmnxLdapServerOperState object is 'out OfService' while the value of the object tmnxLdapServerAdminState is 'inService', make sure that the LDAP server connection parameters are properly configured and the LDAP server is reachable.
Effect	N/A
Recovery	N/A

33 LDP

33.1 vRtrLdpGroupIdMismatch

Table 599: vRtrLdpGroupIdMismatch properties

Property name	Value
Application name	LDP
Event ID	2004
Event name	vRtrLdpGroupIdMismatch
SNMP notification prefix and OID	TIMETRA-LDP-MIB.tmnxLdpNotifications.5
Default severity	minor
Message format string	Apparent mismatch of group IDs - local group ID: *$vRtrLdpNotifyLocalGroupID$*, remote group ID: *$vRtrLdpNotifyRemoteGroupID$*
Cause	N/A
Effect	N/A
Recovery	N/A

33.2 vRtrLdpNgIfStateChange

Table 600: vRtrLdpNgIfStateChange properties

Property name	Value
Application name	LDP
Event ID	2013
Event name	vRtrLdpNgIfStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.3
Default severity	minor
Message format string	Interface instance state changed - vRtrID: *$vRtrID$*, *$interfaceName$*, administrative state: *$vRtrLdpNgIfAdminState$*, operational state: *$vRtrLdpNgIfOperState$*

Property name	Value
Cause	The vRtrLdpNgIfStateChange notification is generated when the LDP interface changes state either administratively or operationally.
Effect	Based on the vRtrLdpNgIfOperDownReason reason code, the system may not be able to accept new requests from peers over this interface.
Recovery	Based on the vRtrLdpNgIfOperDownReason reason code, appropriate configuration changes in LDP may be required.

33.3 vRtrLdpNgInetIfStateChange

Table 601: vRtrLdpNgInetIfStateChange properties

Property name	Value
Application name	LDP
Event ID	2014
Event name	vRtrLdpNgInetIfStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.4
Default severity	minor
Message format string	Sub-interface instance state changed - vRtrID: *$vRtrID$*, *$interface Name$*, administrative state: *$vRtrLdpNgInetIfAdminState$*, operational state: *$vRtrLdpNgInetIfOperState$*
Cause	The vRtrLdpNgInetIfStateChange notification is generated when the LDP sub-interface changes state either administratively or operationally.
Effect	Based on the vRtrLdpNgInetIfOperDownReason reason code, the system may not be able to accept new requests over this interface.
Recovery	Based on the vRtrLdpNgInetIfOperDownReason reason code, appropriate configuration changes in LDP may be required.

33.4 vRtrLdpNgIpv4InstStateChange

Table 602: vRtrLdpNgIpv4InstStateChange properties

Property name	Value
Application name	LDP

Property name	Value
Event ID	2011
Event name	vRtrLdpNgIpv4InstStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.1
Default severity	minor
Message format string	IPv4 Instance state changed - vRtrID: *$vRtrID$*, administrative state: *$vRtrLdpNgGenAdminState$*, operational state: *$vRtrLdp NgGenIPv4OperState$*, reason: *$vRtrLdpNgGenIPv4OperDown Reason$*
Cause	The vRtrLdpNgIpv4InstStateChange is generated when the IPv4 LDP instance changes state operationally as specified by vRtrLdp NgGenIPv4OperState.
Effect	Based on the vRtrLdpNgGenIPv4OperDownReason reason code, the system may not be able to accept new requests from peers.
Recovery	Based on the vRtrLdpNgGenIPv4OperDownReason reason code, appropriate configuration changes in LDP may be required.

33.5 vRtrLdpNgIpv6InstStateChange

Table 603: vRtrLdpNgIpv6InstStateChange properties

Property name	Value
Application name	LDP
Event ID	2012
Event name	vRtrLdpNgIpv6InstStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.2
Default severity	minor
Message format string	IPv6 Instance state changed - vRtrID: *$vRtrID$*, administrative state: *$vRtrLdpNgGenAdminState$*, operational state: *$vRtrLdp NgGenIPv6OperState$*, reason: *$vRtrLdpNgGenIPv6OperDown Reason$*
Cause	The vRtrLdpNgIpv6InstStateChange is generated when the IPv6 LDP instance changes state operationally as specified by vRtrLdp NgGenIPv6OperState.

Property name	Value
Effect	Based on the vRtrLdpNgGenIPv6OperDownReason reason code, the system may not be able to accept new requests from peers.
Recovery	Based on the vRtrLdpNgGenIPv6OperDownReason reason code, appropriate configuration changes in LDP may be required.

33.6 vRtrLdpNgResourceExhaustion

Table 604: vRtrLdpNgResourceExhaustion properties

Property name	Value
Application name	LDP
Event ID	2019
Event name	vRtrLdpNgResourceExhaustion
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.9
Default severity	minor
Message format string	Instance resource exhausted - vRtrID: *$vRtrID$*
Cause	The vRtrLdpNgResourceExhaustion notification is generated when a CPM or data path resource required for FEC resolution is exhausted. The new notification will not be generated if multiple internal event changes occur within a 10 minute interval.
Effect	The system may not be able to accept new requests from peers.
Recovery	Appropriate configuration changes in LDP may be required.

33.7 vRtrLdpNgSessionStateChange

Table 605: vRtrLdpNgSessionStateChange properties

Property name	Value
Application name	LDP
Event ID	2016
Event name	vRtrLdpNgSessionStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.6

Property name	Value
Default severity	minor
Message format string	Session state is *$vRtrLdpNgSessState$*. Overload Notification message is *$vRtrLdpNgSessOverloadDirection$* to/from peer *$vRtrLdpNgPeerLdpId$* with overload state *$vRtrLdpNgSessOverloadState$* for fec type *$vRtrLdpNgSessOverloadFecType$* and sub type fec *$vRtrLdpNgSessOvldFecTypeSubTyp$*
Cause	The vRtrLdpNgSessionStateChange notification is generated when the LDP Overload Notification message is sent to or received from the peer vRtrLdpNgPeerLdpId for the combination of vRtrLdpNgSessOverloadFecType and vRtrLdpNgSessOvldFecTypeSubTyp while vRtrLdpNgSessState remains 'operational'.
Effect	Once the Local LSR has sent the LDP Overload Notification message to the peer vRtrLdpNgPeerLdpId for fec and sub type fec indicated by vRtrLdpNgSessOverloadFecType and vRtrLdpNgSessOvldFecTypeSubTyp and vRtrLdpNgSessOverloadState has the value of 'true', then new Label Mapping Messages received for this peer for the given combination of fec and sub type fec is returned with a Label Release Message. If the Local LSR has received an LDP Overload Notification message from the peer vRtrLdpNgPeerLdpId for fec and sub type fec indicated by vRtrLdpNgSessOverloadFecType and vRtrLdpNgSessOvldFecTypeSubTyp and vRtrLdpNgSessOverloadState has the value of 'true', no new Label Mapping Message for the given combination of fec and sub type fec will be sent to this peer. If the Local LSR has received an LDP Overload Notification message from the peer vRtrLdpNgPeerLdpId for fec and sub type fec indicated by vRtrLdpNgSessOverloadFecType and vRtrLdpNgSessOvldFecTypeSubTyp and vRtrLdpNgSessOverloadState has the value of 'false', then the Local LSR will send all pending and any new Label Mapping Message for the given combination of fec and sub type fec to this peer.
Recovery	In case the Local LSR sent the LDP Overload Notification message to the peer vRtrLdpNgPeerLdpId and vRtrLdpNgSessOverloadState has the value of 'true' for fec and sub type fec indicated by vRtrLdpNgSessOverloadFecType and vRtrLdpNgSessOvldFecTypeSubTyp, then appropriate LDP configuration changes may be required on the Local and/or Remote LSR. Once the Local LSR is not overloaded anymore, an LDP Overload Notification message is sent to the peer vRtrLdpNgPeerLdpId and vRtrLdpNgSessOverloadState has the value of 'false' for given fec and sub type fec.

33.8 vRtrLdpNgSessMaxFecLimitReached

Table 606: vRtrLdpNgSessMaxFecLimitReached properties

Property name	Value
Application name	LDP
Event ID	2018
Event name	vRtrLdpNgSessMaxFecLimitReached
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.8
Default severity	major
Message format string	Number of FECs received from the peer *$vRtrLdpNgPeerAddress$* has reached the maximum value of *$vRtrLdpNgSessParamMaxFec $*. The current operational threshold is *$vRtrLdpNgSessOperMaxFec Threshold$* percent.
Cause	A vRtrLdpNgSessMaxFecLimitReached notification is generated when the number of FEC's accepted from the peer has reached the value specified by vRtrLdpNgSessParamMaxFec. If the current number of FEC's go below the limit but higher than the configured threshold and again start to increase and hit the limit a second time, we will raise a trap if 2 or more minutes have elapsed since the first vRtrLdpNgSess MaxFecLimitReached trap was sent. If any parameter in FEC limit configuration changes and the current number of FEC's are equal to or higher than the limit specified by vRtrLdpPeerMaxFec, then we would always raise the vRtrLdpNgSessMaxFecLimitReached trap.
Effect	When the number of FECs exceed the configured maximum (vRtr LdpNgSessParamMaxFec) it results in any of the following: (1) If vRtr LdpNgSessParamMaxFecLogOnly is set to 'false' and LSR Overload Capability is supported, then Overload procedure will take place. (2) If vRtrLdpNgSessParamMaxFecLogOnly is set to 'false' and LSR Overload Capability is not supported, Label Mapping Message will be returned with Label Release Message. (3) If vRtrLdpNgSessParamMax FecLogOnly is set to 'true', no action will be taken.
Recovery	Appropriate Configuration changes in local or peer LSR will be required.

33.9 vRtrLdpNgSessMaxFecThresChanged

Table 607: vRtrLdpNgSessMaxFecThresChanged properties

Property name	Value
Application name	LDP
Event ID	2017
Event name	vRtrLdpNgSessMaxFecThresChanged
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.7
Default severity	warning
Message format string	Number of FECs received from the peer *$vRtrLdpNgPeerAddress$* has gone *$vRtrLdpNgSessOperThresLevel$* the configured threshold of the maximum value *$vRtrLdpNgSessParamMaxFec$*. The current operational threshold is *$vRtrLdpNgSessOperMaxFecThreshold$* percent.
Cause	A vRtrLdpNgSessMaxFecThresChanged notification is generated when the number of FECs accepted from the peer has exceeded or drops below vRtrLdpNgSessOperMaxFecThreshold percent of the value specified by vRtrLdpNgSessParamMaxFec. New notification will not be generated if multiple internal event change occurs for the same level indicated by vRtrLdpNgSessOperThresLevel during a 2 minute interval. If any parameter in FEC limit configuration changes then we would always raise this trap if current number of FEC's are above the configured threshold or has crossed the threshold downwards. If we remain on or below the configured threshold before and after the configuration changes then no trap would be generated.
Effect	No direct effect but if the peer LSR continues to send further Label Mapping Message, then the number of FECs may exceed the configured maximum (vRtrLdpNgSessParamMaxFec) resulting in the generation of vRtrLdpNgSessMaxFecLimitReached notification.
Recovery	Appropriate Configuration changes in local or peer LSR will be required.

33.10 vRtrLdpNgTargPeerStateChange

Table 608: vRtrLdpNgTargPeerStateChange properties

Property name	Value
Application name	LDP

Property name	Value
Event ID	2015
Event name	vRtrLdpNgTargPeerStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.5
Default severity	minor
Message format string	Targeted peer state changed - vRtrID: *$vRtrID$*, *$vRtrLdpNgPeer Address$*, administrative state: *$vRtrLdpNgTargPeerAdminState$*, operational state: *$vRtrLdpNgTargPeerOperState$*
Cause	The vRtrLdpNgTargPeerStateChange notification is generated when the LDP peer changes state either administratively or operationally.
Effect	Based on the vRtrLdpNgTargPeerOperDownReason reason code, the system may not be able to accept new requests from this peer.
Recovery	Based on the vRtrLdpNgTargPeerOperDownReason reason code, appropriate configuration changes in LDP may be required.

33.11 vRtrLdpStateChange

Table 609: vRtrLdpStateChange properties

Property name	Value
Application name	LDP
Event ID	2001
Event name	vRtrLdpStateChange
SNMP notification prefix and OID	TIMETRA-LDP-MIB.tmnxLdpNotifications.1
Default severity	minor
Message format string	LDP protocol *$vRtrLdpStatus$*d
Cause	The vRtrLdpStateChange notification is generated when the LDP protocol is created or deleted in the router
Effect	N/A
Recovery	N/A

34 LI

34.1 cli_config_io

Table 610: cli_config_io properties

Property name	Value
Application name	LI
Event ID	2115
Event name	cli_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	A valid CLI command was entered in the configuration node.
Effect	Configuration was changed by CLI command.
Recovery	No recovery is required.

34.2 cli_unauth_config_io

Table 611: cli_unauth_config_io properties

Property name	Value
Application name	LI
Event ID	2117
Event name	cli_unauth_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	User has entered configuration command for which he is not authorized.

Property name	Value
Effect	The CLI command was not processed.
Recovery	No recovery is required.

34.3 cli_unauth_user_io

Table 612: cli_unauth_user_io properties

Property name	Value
Application name	LI
Event ID	2116
Event name	cli_unauth_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	User has entered command for which he is not authorized.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

34.4 cli_user_io

Table 613: cli_user_io properties

Property name	Value
Application name	LI
Event ID	2113
Event name	cli_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	A CLI command was entered.

Property name	Value
Effect	A CLI command was processed.
Recovery	No recovery is required.

34.5 cli_user_login

Table 614: cli_user_login properties

Property name	Value
Application name	LI
Event ID	2101
Event name	cli_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	The user was successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required.

34.6 cli_user_login_failed

Table 615: cli_user_login_failed properties

Property name	Value
Application name	LI
Event ID	2103
Event name	cli_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	The user failed authentication.

Property name	Value
Effect	The user access session was not started. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

34.7 cli_user_login_max_attempts

Table 616: cli_user_login_max_attempts properties

Property name	Value
Application name	LI
Event ID	2104
Event name	cli_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.51
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxUserCliLoginMaxAttempts notification is generated when a user attempting to open a CLI sesssion failed to authenticate for more than a maximum allowed number of times in a period of tmnxPassword AttemptsTime minutes. The value of the object tmnxPasswordAttempts Count indicates the maximum number of unsuccessful login attempts allowed. The value of the object tmnxPasswordAttemptsLockout Period indicates the number of minutes the user is locked out if the threshold of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUserName indicates the name of the user attempting to open a CLI session. The value of the object tmnx SecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to open a CLI session.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. A remote access session is terminated.
Recovery	No recovery action is required.

34.8 cli_user_logout

Table 617: cli_user_logout properties

Property name	Value
Application name	LI
Event ID	2102
Event name	cli_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	A user access session was stopped.
Recovery	No recovery is required.

34.9 destinationDisabled

Table 618: destinationDisabled properties

Property name	Value
Application name	LI
Event ID	2014
Event name	destinationDisabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.4
Default severity	minor
Message format string	Mirror destination *$tMirrorDestinationIndex$* is administratively disabled ('shutdown')
Cause	The operator disabled the mirror destination.
Effect	No mirror traffic will egress. Applications using the mirror traffic will not receive any traffic from this destination.
Recovery	The operator intentionally disabled the mirror destination, so no recovery is necessary. Enable the mirror destination to restart mirroring.

34.10 destinationEnabled

Table 619: destinationEnabled properties

Property name	Value
Application name	LI
Event ID	2013
Event name	destinationEnabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.3
Default severity	minor
Message format string	Mirror destination *$tMirrorDestinationIndex$* is administratively enabled ('no shutdown')
Cause	The operator enabled the mirror destination.
Effect	The mirror traffic will egress. Applications using the mirror traffic will receive traffic from this destination.
Recovery	The operator intentionally enabled the mirror destination, so no recovery is necessary.

34.11 ftp_user_login

Table 620: ftp_user_login properties

Property name	Value
Application name	LI
Event ID	2105
Event name	ftp_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	The user was successfully authenticated for login.
Effect	A user access session begins.
Recovery	No recovery is required

34.12 ftp_user_login_failed

Table 621: ftp_user_login_failed properties

Property name	Value
Application name	LI
Event ID	2107
Event name	ftp_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session does not begin. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

34.13 ftp_user_login_max_attempts

Table 622: ftp_user_login_max_attempts properties

Property name	Value
Application name	LI
Event ID	2108
Event name	ftp_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.53
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxLiUserFtpLoginMaxAttempts notification is generated when a Lawful Interception user attempting to connect via FTP failed to authenticate for more than a maximum allowed number of times in a period of tmnxPasswordAttemptsTime minutes. The value of the object tmnxPasswordAttemptsCount indicates the maximum number

Property name	Value
	of unsuccessful login attempts allowed. The value of the object tmnx PasswordAttemptsLockoutPeriod indicates the number of minutes the user is locked out if the threshold of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUser Name indicates the name of the user attempting to connect via FTP. The value of the object tmnxSecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to connect via FTP.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. An FTP session is terminated.
Recovery	No recovery action is required.

34.14 ftp_user_logout

Table 623: ftp_user_logout properties

Property name	Value
Application name	LI
Event ID	2106
Event name	ftp_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ends.
Recovery	No recovery is required

34.15 host_snmp_attempts

Table 624: host_snmp_attempts properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2123
Event name	host_snmp_attempts
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Host *$hostAddress$* is locked out for *$lockoutTime$* minutes since it exceeded the configured threshold of unsuccessful SNMP connection attempts.
Cause	A host (manager IP address) exceded the configured number of access attempts.
Effect	The host is locked out and the router will not respond to the SNMP requests from the host.
Recovery	N/A

34.16 radiusFailed

Table 625: radiusFailed properties

Property name	Value
Application name	LI
Event ID	2124
Event name	radiusFailed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	LI for host failed: *$reason$*
Cause	N/A
Effect	N/A
Recovery	N/A

34.17 sbiBootLiConfig

Table 626: sbiBootLiConfig properties

Property name	Value
Application name	LI
Event ID	2001
Event name	sbiBootLiConfig
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.40
Default severity	major
Message format string	Lawful Intercept (LI) bootup configuration status: *$sliConfigStatus$*. LI separate: *$sbiLiSeparate$*. LI local save: *$sbiLiLocalSave$*. System last booted time: *$sysUpTime$*.
Cause	The bootup LI configuration phase is finished.
Effect	LI configuration will be missing or incomplete if LI configuration phase was not completed successfully.
Recovery	Determine failure cause and restore LI configuration manually or reboot.

34.18 snmp_user_set

Table 627: snmp_user_set properties

Property name	Value
Application name	LI
Event ID	2114
Event name	snmp_user_set
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	SNMP user from *$srcAddr$*> *$vbList$*
Cause	A valid SNMP SET reqest was received.
Effect	The configuration was changed by an SNMP SET operation.
Recovery	No recovery is required.

34.19 sourceDisabled

Table 628: sourceDisabled properties

Property name	Value
Application name	LI
Event ID	2012
Event name	sourceDisabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.2
Default severity	minor
Message format string	LI Mirror source *$tMirrorSourceIndex$* is administratively disabled ('shutdown')
Cause	The operator disabled the LI mirror source
Effect	No traffic from this source will be mirrored. Applications using the mirror traffic will not receive any traffic from this source.
Recovery	The operator intentionally disabled the LI mirror source, so no recovery is required. Enable the LI mirror source to restart mirroring.

34.20 sourceEnabled

Table 629: sourceEnabled properties

Property name	Value
Application name	LI
Event ID	2011
Event name	sourceEnabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.1
Default severity	minor
Message format string	LI Mirror source *$tMirrorSourceIndex$* is administratively enabled ('no shutdown')
Cause	Operator enabled the LI mirror source
Effect	Traffic from this source will be mirrored. Applications using the mirror traffic will receive traffic from this source.

Property name	Value
Recovery	The Operator intentionally enabled the LI mirror source, so no recovery is required. Disable the LI mirror source to stop LI mirroring.

34.21 sourceSapChange

Table 630: sourceSapChange properties

Property name	Value
Application name	LI
Event ID	2018
Event name	sourceSapChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.8
Default severity	minor
Message format string	Lawful Intercept Mirror source *$tMirrorSourceIndex$* associated SAP *$tMirrorSourceSapEncapValue$* has been *$tMirrorSourceChangeType$*
Cause	A SAP associated with the LI mirror source has been modified or deleted.
Effect	Mirrored traffic from this source may be affected in an undesired manner.
Recovery	Modify the configuration of the associated SAP to restore the desired mirrored traffic.

34.22 sourceSubscriberChange

Table 631: sourceSubscriberChange properties

Property name	Value
Application name	LI
Event ID	2019
Event name	sourceSubscriberChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.9
Default severity	minor

Property name	Value
Message format string	Mirroring for Lawful Intercept mirror source *$tMirrorSourceIndex$* subscriber "*$tMirrorSourceSubIdent$*" has been *$tMirrorSourceChangeType$*
Cause	A subscriber associated with the LI mirror source has been activated, deactivated, modified, or deleted.
Effect	Mirrored traffic from this source may be affected in an undesired manner.
Recovery	Modify the configuration of the associated subscriber to restore the desired mirrored traffic.

34.23 ssh_user_login

Table 632: ssh_user_login properties

Property name	Value
Application name	LI
Event ID	2109
Event name	ssh_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	The user was successfully authenticated for login.
Effect	A user access session begins.
Recovery	No recovery is required

34.24 ssh_user_login_failed

Table 633: ssh_user_login_failed properties

Property name	Value
Application name	LI
Event ID	2111

Property name	Value
Event name	ssh_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session does not begin. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

34.25 ssh_user_login_max_attempts

Table 634: ssh_user_login_max_attempts properties

Property name	Value
Application name	LI
Event ID	2112
Event name	ssh_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.52
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxLiUserSshLoginMaxAttempts notification is generated when a Lawful Interception user attempting to connect via SSH failed to authenticate for more than a maximum allowed number of times in a period of tmnxPasswordAttemptsTime minutes. The value of the object tmnxPasswordAttemptsCount indicates the maximum number of unsuccessful login attempts allowed. The value of the object tmnx PasswordAttemptsLockoutPeriod indicates the number of minutes the user is locked out if the threshold of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUserName indicates the name of the user attempting to connect via SSH. The value of the object tmnxSecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to connect via SSH.

Property name	Value
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. An SSH session is terminated.
Recovery	No recovery action is required.

34.26 ssh_user_logout

Table 635: ssh_user_logout properties

Property name	Value
Application name	LI
Event ID	2110
Event name	ssh_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ends.
Recovery	No recovery is required

34.27 ssiSaveConfigFailed

Table 636: ssiSaveConfigFailed properties

Property name	Value
Application name	LI
Event ID	2203
Event name	ssiSaveConfigFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.3
Default severity	critical
Message format string	Lawful Intercept configuration file write failed: *$fileName$ $reason$*

Property name	Value
Cause	The save config failed event is generated when the saving of configuration is stopped due to errors.
Effect	Configuration file could not be saved.
Recovery	No recovery is necessary.

34.28 ssiSaveConfigSucceeded

Table 637: ssiSaveConfigSucceeded properties

Property name	Value
Application name	LI
Event ID	2202
Event name	ssiSaveConfigSucceeded
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.2
Default severity	major
Message format string	Lawful Intercept Configuration file saved to: *$fileName$*
Cause	The save config succeeded event is generated when the saving of configuration finishes without errors.
Effect	Configuration file was saved.
Recovery	No recovery is necessary.

34.29 ssiSyncConfigFailed

Table 638: ssiSyncConfigFailed properties

Property name	Value
Application name	LI
Event ID	2213
Event name	ssiSyncConfigFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.15
Default severity	major

Property name	Value
Message format string	Synchronization of Lawful Intercept configuration files failed
Cause	The sync config failed event is generated when the synchronization of configuration files is stopped due to errors.
Effect	Configuration files are not synchronized.
Recovery	No recovery is necessary.

34.30 ssiSyncConfigOK

Table 639: ssiSyncConfigOK properties

Property name	Value
Application name	LI
Event ID	2212
Event name	ssiSyncConfigOK
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.14
Default severity	warning
Message format string	Lawful Intercept configuration files have been successfully synchronized
Cause	The synchronize config succeeded event is generated when the synchronization of configuration files finishes without errors.
Effect	Configuration files synchronized.
Recovery	No recovery is necessary.

34.31 tMirrorDestinationChangeReject

Table 640: tMirrorDestinationChangeReject properties

Property name	Value
Application name	LI
Event ID	2023
Event name	tMirrorDestinationChangeReject

Property name	Value
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.14
Default severity	minor
Message format string	An attempt was blocked to modify mirror destination *$tMirror DestinationIndex$* that is being referenced by Lawful Intercept
Cause	An operator is trying to modify mirror destination that cannot currently be changed because the destination is being used for mirroring.
Effect	The change is not allowed.
Recovery	The mirror destination can only be modified after LI actions are cleared.

34.32 tMirrorFilterAssignToItfWarn

Table 641: tMirrorFilterAssignToItfWarn properties

Property name	Value
Application name	LI
Event ID	2030
Event name	tMirrorFilterAssignToItfWarn
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.19
Default severity	minor
Message format string	*$tMirrorFilterType$* filter *$tMirrorFilterId$* , which is referred to by Lawful Intercept has been applied on *$tMirrorFilterDirection$* to interface *$t MirrorFilterIfName$* (IfIndex *$tMirrorFilterIfIndex$*)
Cause	A filter that is being used for mirroring has been applied to a SDP. This assignment was allowed, but might cause traffic from this SDP to show up in the mirror destination.
Effect	N/A
Recovery	No recovery required.

34.33 tMirrorFilterAssignToSapWarn

Table 642: tMirrorFilterAssignToSapWarn properties

Property name	Value
Application name	LI
Event ID	2028
Event name	tMirrorFilterAssignToSapWarn
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.17
Default severity	minor
Message format string	*$tMirrorFilterType$* filter *$tMirrorFilterId$* , which is referred to by Lawful Intercept has been applied on *$tMirrorFilterDirection$* to SAP *$tMirror FilterSapEncapValue$* in service *$tMirrorFilterSvcId$*
Cause	A filter that is being used for mirroring has been applied to a SAP. This assignment was allowed, but might cause traffic from this SAP to show up in the mirror destination.
Effect	N/A
Recovery	No recovery required.

34.34 tMirrorFilterAssignToSdpWarn

Table 643: tMirrorFilterAssignToSdpWarn properties

Property name	Value
Application name	LI
Event ID	2029
Event name	tMirrorFilterAssignToSdpWarn
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.18
Default severity	minor
Message format string	*$tMirrorFilterType$* filter *$tMirrorFilterId$* , which is referred to by Lawful Intercept has been applied on *$tMirrorFilterDirection$* to SDP *$tMirror FilterSdpBindId$* in service *$tMirrorFilterSvcId$*
Cause	A filter that is being used for mirroring has been applied to a SDP. This assignment was allowed, but might cause traffic from this SDP to show up in the mirror destination.

Property name	Value
Effect	N/A
Recovery	No recovery required.

34.35 tMirrorLiNat64SubOperStateCh

Table 644: tMirrorLiNat64SubOperStateCh properties

Property name	Value
Application name	LI
Event ID	2036
Event name	tMirrorLiNat64SubOperStateCh
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.26
Default severity	minor
Message format string	The state of LI mirror source *$tMirrorSourceIndex$* LSN NAT64 subscriber (*$vRtrID$*, *$tMirrorLiNatLsnSubAddr$*/ *$tMirrorLiNatLsnSubPrefixLength$*) changed to *$tMirrorLiNat64SubOperState$*
Cause	The tMirrorLiNatLsnSubOperStateCh notification is sent when the value of the object tMirrorLiNat64SubOperState changes. This is related to the state of the ISA MDA where the forwarding entry is located, or the availability of resources on that MDA.
Effect	The corresponding inward bound packets are dropped while the operational status is 'down'.
Recovery	If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.

34.36 tMirrorLiNatL2awSubOperStateCh

Table 645: tMirrorLiNatL2awSubOperStateCh properties

Property name	Value
Application name	LI
Event ID	2035
Event name	tMirrorLiNatL2awSubOperStateCh

Property name	Value
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.25
Default severity	minor
Message format string	The state of LI mirror source *$tMirrorSourceIndex$* l2-aware subscriber *$tMirrorLiNatL2awSubIdent$* changed to *$tMirrorLiNatL2awSubOperState$*
Cause	The tMirrorLiNatL2awSubOperStateCh notification is sent when the value of the object tMirrorLiNatL2awSubOperState changes. This is related to the state of the ISA MDA where the forwarding entry is located, the availability of resources on that MDA, or the instantiation of the subscriber.
Effect	The corresponding inward bound packets are dropped while the operational status is 'down'.
Recovery	If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.

34.37 tMirrorLiNatLsnSubOperStateCh

Table 646: tMirrorLiNatLsnSubOperStateCh properties

Property name	Value
Application name	LI
Event ID	2034
Event name	tMirrorLiNatLsnSubOperStateCh
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.24
Default severity	minor
Message format string	The state of LI mirror source *$tMirrorSourceIndex$* LSN subscriber (*$vRtrID$*, *$tMirrorLiNatLsnSubAddr$*/ *$tMirrorLiNatLsnSubPrefixLength$*) changed to *$tMirrorLiNatLsnSubOperState$*
Cause	The tMirrorLiNatLsnSubOperStateCh notification is sent when the value of the object tMirrorLiNatLsnSubOperState changes. This is related to the state of the ISA MDA where the forwarding entry is located, or the availability of resources on that MDA.
Effect	The corresponding inward bound packets are dropped while the operational status is 'down'.

Property name	Value
Recovery	If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.

34.38 tMirrorSourceFilterAssignReject

Table 647: tMirrorSourceFilterAssignReject properties

Property name	Value
Application name	LI
Event ID	2022
Event name	tMirrorSourceFilterAssignReject
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.13
Default severity	minor
Message format string	An attempt was blocked to modify a filter-assignment of a filter that is being referred by Lawful Intercept. *$tMirrorSourceFilterDescr$*
Cause	An operator is trying to modify a filter assignment of a filter that cannot currently be changed because the filter is being used for mirroring.
Effect	The change is disallowed
Recovery	The filter can only be replaced after LI actions are cleared.

34.39 tMirrorSourceFilterAssignWarn

Table 648: tMirrorSourceFilterAssignWarn properties

Property name	Value
Application name	LI
Event ID	2027
Event name	tMirrorSourceFilterAssignWarn
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.16
Default severity	minor

Property name	Value
Message format string	A filter referred to by Lawful Intercept has been assigned in a context where it may be overruled. *$tMirrorSourceFilterDescr$*
Cause	A filter that is being used for mirroring was assigned in a context where it maybe overruled. Filter assignments scheduled by a Time-Of-Day (TOD) Suite take precedence over statically configured filter assignments. There is currently no such overruling filter assignment scheduled, but it may be created in the future.
Effect	None, as long as no overruling filter assignment is created, and is activated.
Recovery	No recovery required. The risk can be eliminated either by creating an identical assignment in the TOD Suite, with the highest priority, or by removing the TOD Suite assignment from the SAP altogether.

34.40 tMirrorSourceFilterOverruled

Table 649: tMirrorSourceFilterOverruled properties

Property name	Value
Application name	LI
Event ID	2026
Event name	tMirrorSourceFilterOverruled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.15
Default severity	minor
Message format string	A filter-assignment of a filter that is being referred by Lawful Intercept was overruled. *$tMirrorSourceFilterDescr$*
Cause	An assignment of a filter that is being used for mirroring was overruled. Filter assignments scheduled by a Time-Of-Day (TOD) Suite take precedence over statically configured filter assignments.
Effect	If the overruling filter assignment refers to a filter that is not used for mirroring, mirror data will be lost.
Recovery	Either the overruling filter assignments can be changed to participate in the intended mirroring, or the TOD suite or the SAP configuration can be modified to prevent this situation.

34.41 tMirrorSourceIPFltrChangeReject

Table 650: tMirrorSourceIPFltrChangeReject properties

Property name	Value
Application name	LI
Event ID	2020
Event name	tMirrorSourceIPFltrChangeReject
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.10
Default severity	minor
Message format string	An attempt was blocked to modify filter-entry *$tMirrorSourceFilterEntry Id$* of IP filter *$tMirrorSourceFilterId$* which is being referred to by Lawful Intercept (mirror-source *$tMirrorSourceIndex$*)
Cause	An operator tried to modify a filter or a filter-entry of a filter that cannot currently be changed because the filter is being used for mirroring.
Effect	The change was blocked.
Recovery	Modifying the filter is only allowed when it is not being referred by any LI action.

34.42 tMirrorSourceIPv6FltrChangeRej

Table 651: tMirrorSourceIPv6FltrChangeRej properties

Property name	Value
Application name	LI
Event ID	2033
Event name	tMirrorSourceIPv6FltrChangeRej
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.23
Default severity	minor
Message format string	An attempt was blocked to modify filter-entry *$tMirrorSourceFilterEntry Id$* of IPv6 filter *$tMirrorSourceFilterId$* which is being referred to by Lawful Intercept (mirror-source *$tMirrorSourceIndex$*)
Cause	The tMirrorSourceIPv6FltrChangeRej event is generated when an operator is trying to modify a filter or a filter-entry of a filter that cannot currently be changed because the filter is being used for mirrorring.

Property name	Value
Effect	The change was blocked.
Recovery	Modifying the filter is only allowed when it is not being referred by any LI action.

34.43 tMirrorSourceLiFilterChanged

Table 652: tMirrorSourceLiFilterChanged properties

Property name	Value
Application name	LI
Event ID	2031
Event name	tMirrorSourceLiFilterChanged
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.20
Default severity	minor
Message format string	A filter which is being referenced by Lawful Intercept has been modified. *$tMirrorSourceFilterDescr$*
Cause	This notification may be triggered only if LI filter lock has been overruled, and one of the following actions has been done: 1) a filter referenced by LI has been deleted. 2) one of the parameters (default-action, scope) of a filter which is referenced by LI has been changed. 3) a filter which is referenced by LI has been overwritten. 4) new entry has been created for a filter which is referenced by LI. 5) an entry of a filter which is referenced by LI has been activated. 6) an entry has been removed from a filter which is referenced by LI. 7) an entry of a filter which is referenced by LI has been renumbered. 8) one of the parameters of an entry in a filter which is referenced by LI has been changed.
Effect	Since a filter which is referenced by LI (or its parameter) has been modified, the mirrored traffic may be changed.
Recovery	N/A

34.44 tMirrorSourceLiSubProblem

Table 653: tMirrorSourceLiSubProblem properties

Property name	Value
Application name	LI
Event ID	2032
Event name	tMirrorSourceLiSubProblem
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.21
Default severity	minor
Message format string	Traffic for for Lawful Intercept mirror source *$tMirrorSourceIndex$* subscriber *$tMirrorSourceSubIdent$* on SAP *$tMirrorNotifyLiSapEncapValue$* in service *$tMirrorNotifyLiSvcId$* could not be intercepted -- *$tMirrorNotifyLiDescription$*
Cause	Detailed information about the exact cause of the notification is available in the object tMirrorNotifyLiDescription. [EFFECT] Traffic of a subscriber subject to Lawful Intercept is not intercepted.
Effect	N/A
Recovery	N/A

34.45 tMirrorSourceMacFltrChangeReject

Table 654: tMirrorSourceMacFltrChangeReject properties

Property name	Value
Application name	LI
Event ID	2021
Event name	tMirrorSourceMacFltrChangeReject
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.12
Default severity	minor
Message format string	An attempt was blocked to modify filter-entry *$tMirrorSourceFilterEntryId$* of Mac filter *$tMirrorSourceFilterId$* which is being referred to by Lawful Intercept (mirror-source *$tMirrorSourceIndex$*)
Cause	An operator tried to modify a filter or a filter-entry of a filter that cannot currently be changed because the filter is being used for mirroring.

Property name	Value
Effect	The change was blocked.
Recovery	Modifying the filter is only allowed when it is not being referred by any LI action.

34.46 tmnxClear

Table 655: tmnxClear properties

Property name	Value
Application name	LI
Event ID	2300
Event name	tmnxClear
SNMP notification prefix and OID	TIMETRA-CLEAR-MIB.tmnxClearNotifications.1
Default severity	indeterminate
Message format string	Clear function *$tmnxClearName$* has been run with parameters: *$tmnxClearParams$*. The completion result is: *$tmnxClearResult$*. Additional error text, if any, is: *$tmnxClearErrorText$*
Cause	The tmnxClear notification is generated to report the results of the clear function that was run as a result of setting tmnxClearAction to 'do Action'.
Effect	If successful, a managed object has been cleared.
Recovery	If the clear action was not successful, make sure the object to be cleared exists and the clear function parameters are correct.

34.47 tmnxConfigCreate

Table 656: tmnxConfigCreate properties

Property name	Value
Application name	LI
Event ID	2207
Event name	tmnxConfigCreate
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9

Property name	Value
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* managed object created
Cause	A tmnxConfigCreate notification is generated when a new row entry is created in one of the MIB tables. It can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

34.48 tmnxConfigDelete

Table 657: tmnxConfigDelete properties

Property name	Value
Application name	LI
Event ID	2208
Event name	tmnxConfigDelete
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.10
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* managed object deleted
Cause	A tmnxConfigDelete notification is generated when an existing row entry in one of the MIB tables is deleted. It can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

34.49 tmnxConfigModify

Table 658: tmnxConfigModify properties

Property name	Value
Application name	LI
Event ID	2206

Property name	Value
Event name	tmnxConfigModify
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.8
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* configuration modified
Cause	A tmnxConfigModify notification is generated when a configuration attribute associated with a row entry in a MIB table is modified. It can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

34.50 tmnxStateChange

Table 659: tmnxStateChange properties

Property name	Value
Application name	LI
Event ID	2209
Event name	tmnxStateChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.11
Default severity	warning
Message format string	Status of *$tmnxNotifyObjectName$* changed administrative state: *$tmnxNotifyRowAdminState$*, operational state: *$tmnxNotifyRowOperState$*
Cause	A tmnxStateChange notification is generated when there is a change in either the adminstrative or operational state of a MIB table entry.
Effect	N/A
Recovery	No recovery is necessary.

35 LLDP

35.1 lldpRemTablesChange

Table 660: lldpRemTablesChange properties

Property name	Value
Application name	LLDP
Event ID	2001
Event name	lldpRemTablesChange
SNMP notification prefix and OID	LLDP-MIB.lldpRemTablesChange.1
Default severity	minor
Message format string	LLDP stats remote table has been updated
Cause	N/A
Effect	N/A
Recovery	N/A

36 LMP

36.1 tmnxLmpVRtrControlChannelState

Table 661: tmnxLmpVRtrControlChannelState properties

Property name	Value
Application name	LMP
Event ID	2005
Event name	tmnxLmpVRtrControlChannelState
SNMP notification prefix and OID	TIMETRA-LMP-MIB.tmnxLmpNotification.5
Default severity	minor
Message format string	Control channel *$tmnxLmpVRtrCcId$* on peer *$tmnxLmpVRtrPeer NodeId$* is *$tmnxLmpVRtrCcOperState$*.
Cause	The tmnxLmpVRtrControlChannelState notification is generated when a control channel transitions to or from the 'up (1)' operational state.
Effect	If no control channels to the peer-node are up, the related TE links cannot be used to set up new GMPLS label-switched paths (LSPs).
Recovery	Ensure the control channel peer-interface is reachable.

36.2 tmnxLmpVRtrDbLinkPropMismatch

Table 662: tmnxLmpVRtrDbLinkPropMismatch properties

Property name	Value
Application name	LMP
Event ID	2003
Event name	tmnxLmpVRtrDbLinkPropMismatch
SNMP notification prefix and OID	TIMETRA-LMP-MIB.tmnxLmpNotification.3
Default severity	minor

Property name	Value
Message format string	DB link *$tmnxLmpVRtrDbLinkId$* detected property mismatch with remote DB link *$tmnxLmpVRtrDbLinkRemoteId$*.
Cause	The tmnxLmpVRtrDbLinkPropMismatch notification is generated when a DB link property mismatch is detected on the node. This notification is only generated the first time a mismatch is detected.
Effect	The DB link is operationally down when a mismatch is detected.
Recovery	Ensure the DB link configuration between the local node and the peer node is consistent.

36.3 tmnxLmpVRtrDbLinkPropMismatchClr

Table 663: tmnxLmpVRtrDbLinkPropMismatchClr properties

Property name	Value
Application name	LMP
Event ID	2004
Event name	tmnxLmpVRtrDbLinkPropMismatchClr
SNMP notification prefix and OID	TIMETRA-LMP-MIB.tmnxLmpNotification.4
Default severity	minor
Message format string	DB link *$tmnxLmpVRtrDbLinkId$* cleared property mismatch with remote DB link *$tmnxLmpVRtrDbLinkRemoteId$*.
Cause	The tmnxLmpVRtrDbLinkPropMismatchClr notification is generated when the DB link property mismatch is cleared.
Effect	The DB link can now service traffic.
Recovery	There is no recovery required for this notification.

36.4 tmnxLmpVRtrTeLinkPropMismatch

Table 664: tmnxLmpVRtrTeLinkPropMismatch properties

Property name	Value
Application name	LMP
Event ID	2001

Property name	Value
Event name	tmnxLmpVRtrTeLinkPropMismatch
SNMP notification prefix and OID	TIMETRA-LMP-MIB.tmnxLmpNotification.1
Default severity	minor
Message format string	TE link *$tmnxLmpVRtrTeLinkId$* detected property mismatch on peer *$tmnxLmpVRtrTeLinkPeerNodeId$* with remote TE link *$tmnxLmpVRtrTeLinkRemoteId$*.
Cause	The tmnxLmpVRtrTeLinkPropMismatch notification is generated when a TE link property mismatch is detected on the node. This notification is only generated the first time a mismatch is detected.
Effect	The TE link is operationally down when a mismatch is detected.
Recovery	Ensure the TE link configuration between the local node and the peer node is consistent.

36.5 tmnxLmpVRtrTeLinkPropMismatchClr

Table 665: tmnxLmpVRtrTeLinkPropMismatchClr properties

Property name	Value
Application name	LMP
Event ID	2002
Event name	tmnxLmpVRtrTeLinkPropMismatchClr
SNMP notification prefix and OID	TIMETRA-LMP-MIB.tmnxLmpNotification.2
Default severity	minor
Message format string	TE link *$tmnxLmpVRtrTeLinkId$* cleared property mismatch on peer *$tmnxLmpVRtrTeLinkPeerNodeId$* with remote TE link *$tmnxLmpVRtrTeLinkRemoteId$*.
Cause	The tmnxLmpVRtrTeLinkPropMismatchClr notification is generated when a TE link property mismatch is cleared.
Effect	The TE link can now service traffic.
Recovery	There is no recovery required for this notification.

36.6 tmnxLmpVRtrTeLinkState

Table 666: tmnxLmpVRtrTeLinkState properties

Property name	Value
Application name	LMP
Event ID	2006
Event name	tmnxLmpVRtrTeLinkState
SNMP notification prefix and OID	TIMETRA-LMP-MIB.tmnxLmpNotification.6
Default severity	minor
Message format string	TE link *$tmnxLmpVRtrTeLinkId$* is *$tmnxLmpVRtrTeLinkOperState$*.
Cause	The tmnxLmpVRtrTeLinkState notification is generated when a TE link's operational state changes.
Effect	When tmnxLmpVRtrTeLinkOperState is not 'up (1)', no new GMPLS LSPs can be set up using this TE link.
Recovery	When tmnxLmpVRtrTeLinkOperState is 'degraded (5)', bring up at least one control channel with the relevant peer node.

37 LOGGER

37.1 STARTED

Table 667: STARTED properties

Property name	Value
Application name	LOGGER
Event ID	2001
Event name	STARTED
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Event collector *$taskName$* started
Cause	An event log collector process was started.
Effect	Application events will be collected, filtered, and distributed, as configured.
Recovery	No recovery; not applicable.

37.2 tmnxClear

Table 668: tmnxClear properties

Property name	Value
Application name	LOGGER
Event ID	2010
Event name	tmnxClear
SNMP notification prefix and OID	TIMETRA-CLEAR-MIB.tmnxClearNotifications.1
Default severity	indeterminate
Message format string	Clear function *$tmnxClearName$* has been run with parameters: *$tmnxClearParams$*. The completion result is: *$tmnxClearResult$*. Additional error text, if any, is: *$tmnxClearErrorText$*

Property name	Value
Cause	The tmnxClear notification is generated to report the results of the clear function that was run as a result of setting tmnxClearAction to 'do Action'.
Effect	If successful, the managed object was cleared.
Recovery	If failed, check that the managed object exists or that the clear function parameters are correct.

37.3 tmnxLogAccountingDataLoss

Table 669: tmnxLogAccountingDataLoss properties

Property name	Value
Application name	LOGGER
Event ID	2014
Event name	tmnxLogAccountingDataLoss
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.10
Default severity	major
Message format string	Accounting data loss occured for *$subject$*.
Cause	An accounting file was still being written to when the next collection interval ended.
Effect	A tmnxLogAccountingDataLoss notification is generated when an accounting file is still being written to when the next collection interval ends. The collection of statistics for the past interval is immediately stopped and collection is started for the next interval. There are missing records in the file for this past interval.
Recovery	N/A

37.4 tmnxLogAdminLocFailed

Table 670: tmnxLogAdminLocFailed properties

Property name	Value
Application name	LOGGER
Event ID	2006

Property name	Value
Event name	tmnxLogAdminLocFailed
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.2
Default severity	major
Message format string	Possible messages: • Compact flash location is not available for *$subject$*. Backup location, if any, will be used. • Compact flash location cf *$tmnxLogFileIdAdminLocation$* is not available for *$subject$*. Backup location, if any, will be used.
Cause	Generated when the specified admin cflash is not available. Indicates that an alternative backup location, if specified, will be used.
Effect	N/A
Recovery	N/A

37.5 tmnxLogBackupLocFailed

Table 671: tmnxLogBackupLocFailed properties

Property name	Value
Application name	LOGGER
Event ID	2007
Event name	tmnxLogBackupLocFailed
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.3
Default severity	major
Message format string	Compact flash backup location cf *$tmnxLogFileIdBackupLoc$* is not available for *$subject$* .File destination creation failed
Cause	Generated when the specified backup cflash is not available.
Effect	No log or billing file was created on either the admin or backup cflash.
Recovery	N/A

37.6 tmnxLogEventOverrun

Table 672: tmnxLogEventOverrun properties

Property name	Value
Application name	LOGGER
Event ID	2017
Event name	tmnxLogEventOverrun
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.12
Default severity	major
Message format string	*$tmnxLogThrottledEvents$ $tmnxLogThrottledEventID$* events were dropped because of logger input queue overrun.
Cause	A tmnxLogEventOverrun notification is generated at the end of the overrun throttling interval when one or more events of the type specified by tmnxLogThrottledEventID were dropped because the logger input stream's input queue limit was exceeded. The overrun throttling interval begins when the input queue limit is first exceeded and ends when the number of events in the input queue has dropped below an internal low watermark. At that point a tmnxLogEventOverrun notification is generated for each event type that had one or more events dropped because of the input queue overrun. The number of dropped events is specified by tmnxLogThrottledEvents.
Effect	Logger events have been dropped and were not sent to any log destination. tmnxEventDropCount has been incremented for each event dropped because of input queue overrun.
Recovery	The specific event information of dropped events cannot be recovered. The frequency of input queue overruns can be lessened by configuring as few event logs as possible, especially those going to remote destinations such as file, syslog and snmp notification logs

37.7 tmnxLogEventThrottled

Table 673: tmnxLogEventThrottled properties

Property name	Value
Application name	LOGGER
Event ID	2012
Event name	tmnxLogEventThrottled

Property name	Value
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.8
Default severity	major
Message format string	*$tmnxLogThrottledEvents$ $tmnxLogThrottledEventID$* events were dropped in the last event throttling interval.
Cause	A tmnxLogEventThrottled notification is generated at the end of the throttling interval when one or more events are dropped because the throttling limit was reached for that interval.
Effect	N/A
Recovery	N/A

37.8 tmnxLogFileDeleted

Table 674: tmnxLogFileDeleted properties

Property name	Value
Application name	LOGGER
Event ID	2009
Event name	tmnxLogFileDeleted
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.5
Default severity	minor
Message format string	Log file *$tmnxLogFileDeletedName$* on compact flash cf *$tmnxLogFileDeletedLocation$* has been deleted
Cause	Generated when a closed event log or accounting policy file has been deleted as part of the space contention cleanup.
Effect	N/A
Recovery	N/A

37.9 tmnxLogFileRollover

Table 675: tmnxLogFileRollover properties

Property name	Value
Application name	LOGGER
Event ID	2008
Event name	tmnxLogFileRollover
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.4
Default severity	major
Message format string	Log file *$tmnxLogFileIdPathName$* on compact flash cf *$tmnxLogFile IdOperLocation$* has been rolled over
Cause	Generated when an event log or accounting policy file's rollover time has expired.
Effect	The file located as indicated by the value of tmnxLogFileIdOper Location is closed and a new file is created as specified by tmnxLogFile IdAdminLocation and tmnxLogFileIdBackupLoc.
Recovery	No recovery is necessary.

37.10 tmnxLogOnlyEventOverrun

Table 676: tmnxLogOnlyEventOverrun properties

Property name	Value
Application name	LOGGER
Event ID	2018
Event name	tmnxLogOnlyEventOverrun
SNMP notification prefix and OID	N/A
Default severity	major
Message format string	*$tmnxLogOnlyOverrunEvents$ $tmnxLogOnlyOverrunEventName$* log-only (L) events were dropped because the logger input queue was overrun.
Cause	A tmnxLogOnlyEventOverrun notification is generated at the end of the overrun throttling interval when one or more log-only events of the type specified by tmnxLogOnlyOverrunEventName were dropped because the logger input stream's input queue limit was exceeded. The overrun

Property name	Value
	throttling interval begins when the input queue limit is first exceeded and ends when the number of events in the input queue has dropped below an internal low watermark. At that point a tmnxLogOnlyEvent Overrun notification is generated for each log-only event type that had one or more events dropped because of the input queue overrun. The number of dropped events is specified by tmnxLogOnlyOverrunEvents.
Effect	Logger events have been dropped and were not sent to any log destination. tmnxEventDropCount has been incremented for each event dropped because of input queue overrun.
Recovery	The specific event information of dropped events cannot be recovered. The frequency of input queue overruns can be lessened by configuring as few event logs as possible, especially those going to remote destinations such as file, syslog and snmp notification logs

37.11 tmnxLogOnlyEventThrottled

Table 677: tmnxLogOnlyEventThrottled properties

Property name	Value
Application name	LOGGER
Event ID	2016
Event name	tmnxLogOnlyEventThrottled
SNMP notification prefix and OID	N/A
Default severity	major
Message format string	*$tmnxLogOnlyThrottledEvents$ $tmnxLogOnlyThrottledEventName$* log-only (L) events were dropped in the last event throttling interval.
Cause	One or more log-only events were dropped because the throttling limit was reached for that interval.
Effect	A tmnxLogOnlyEventThrottled event is generated at the end of the throttling interval when one or more log-only events are dropped because the throttling limit was reached for that interval.
Recovery	N/A

37.12 tmnxLogSpaceContention

Table 678: tmnxLogSpaceContention properties

Property name	Value
Application name	LOGGER
Event ID	2005
Event name	tmnxLogSpaceContention
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.1
Default severity	major
Message format string	Space contention occurred on compact flash cf *$cFlashId$* during I/O for *$subject$*.
Cause	Generated when space contention occurs on the compact flash where a log or billing file creation is being attempted. Space contention exists if: Insufficient space is available on the compact flash to create a file of the same size as the file being rolled over. The first file of this type is being created and less than 10% of the total compact flash space is available. A write operation on a log or billing file is denied due to lack of space.
Effect	N/A
Recovery	N/A

37.13 tmnxLogTraceError

Table 679: tmnxLogTraceError properties

Property name	Value
Application name	LOGGER
Event ID	2002
Event name	tmnxLogTraceError
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.7
Default severity	critical
Message format string	*$tmnxLogTraceErrorTitle$*: *$tmnxLogTraceErrorMessage$*
Cause	A critical level trace error has been detected by the software.
Effect	N/A

Property name	Value
Recovery	N/A

37.14 tmnxStdEventsReplayed

Table 680: tmnxStdEventsReplayed properties

Property name	Value
Application name	LOGGER
Event ID	2015
Event name	tmnxStdEventsReplayed
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.11
Default severity	major
Message format string	Events *$tmnxStdReplayStartEvent$* to *$tmnxStdReplayEndEvent$* from *$subject$* have been resent to SNMP notification target address *$tmnxStdDestAddr$*. The first event with no route to the target address was *$tmnxStdReplayStart$*.
Cause	An SNMP trap target address was added to the route table following a period when a route to that address was not available.
Effect	A tmnxStdEventsReplayed notification is generated when an SNMP trap target address is added to the RTM (tmnxVRtrID) following a period when the address had been removed. The value of tmnxStd ReplayStartEvent is the SNMP notification request ID of the first event that was replayed. The value of tmnxStdReplayEndEvent is the SNMP notification request ID of the last missed event that was replayed. The value of tmnxStdReplayStart is the request ID of the first event for which there was no route to the trap target address.
Recovery	N/A

37.15 tmnxSysLogTargetProblem

Table 681: tmnxSysLogTargetProblem properties

Property name	Value
Application name	LOGGER
Event ID	2013

Property name	Value
Event name	tmnxSysLogTargetProblem
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.9
Default severity	major
Message format string	Problem encountered when trying to reach the destination specified in syslog *$tmnxSysLogTargetId$* : *$tmnxSysLogTargetProblemDescr$*.
Cause	An event could not be delivered to the destination specified for the syslog.
Effect	A tmnxSysLogTargetProblem notification is generated when a problem is encountered when trying to deliver data to the syslog destination identfied by the tmnxSysLogTargetId.
Recovery	N/A

37.16 tmnxTestEvent

Table 682: tmnxTestEvent properties

Property name	Value
Application name	LOGGER
Event ID	2011
Event name	tmnxTestEvent
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.6
Default severity	indeterminate
Message format string	Test event has been generated with system object identifier *$sys ObjectID$* System description: *$sysDescr$*
Cause	The tmnxTestEvent notification is generated when the object tmnx EventTest is set to a value of 'doAction' or the tools>perform>log>test-event CLI command has been entered. This event can be used to test that remote log destinations such as syslog and snmp trap destinations are configured correctly.
Effect	A tmnxTestEvent is generated.
Recovery	If the test event is not received by the log destination, verify that syslog and snmp trap destinations are configured correctly and that the interface link between the system and the remote receiver is up.

38 MC_REDUNDANCY

38.1 srrpPacketDiscarded

Table 683: srrpPacketDiscarded properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2025
Event name	srrpPacketDiscarded
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Discarded SRRP packet from *$tmnxMcPeerSrcIpAddr$* because *$srrp PacketDiscardReason$*
Cause	The following checks are performed on an incoming SRRP packet 1. verify that the IP TTL is 255. 2. verify the SRRP version. 3. verify that the received packet length is greater than or equal to the SRRP header. 4. verify the SRRP checksum. 5. perform authentication specified by Auth Type. If any one of the above checks fail, the receiver must discard the packet and log the event.
Effect	N/A
Recovery	N/A

38.2 tMcPeerIPsecTnlGrpMasterStateChg

Table 684: tMcPeerIPsecTnlGrpMasterStateChg properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2035
Event name	tMcPeerIPsecTnlGrpMasterStateChg
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.34

Property name	Value
Default severity	warning
Message format string	Master state for the multi-chassis ipsec peer *$tmnxMcPeerIpAddr$* tunnel-group *$tMcPeerIPsecTnlGrpId$* changed from *$tMcPeerIPsec TnlGrpMasterStateOld$* to *$tMcPeerIPsecTnlGrpMasterState$* because *$tMcPeerIPsecTnlGrpMasterStateChR$*
Cause	The notification tMcPeerIPsecTnlGrpMasterStateChg is generated whenever mastership election state of a tunnel-group changes.
Effect	This trap is informational. The effects associated with this notification depend upon the new state of the tunnel-group. For example, when a tunnel-group becomes master it will begin attracting traffic towards its chassis and will begin to manage IKE sessions for all IPsec tunnels in that tunnel-group.
Recovery	No recovery actions are required, although unexpected state transitions often indicate causal fault conditions which may require investigation.

38.3 tMcPeerIPsecTnlGrpProtStatusChg

Table 685: tMcPeerIPsecTnlGrpProtStatusChg properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2036
Event name	tMcPeerIPsecTnlGrpProtStatusChg
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.35
Default severity	warning
Message format string	Protection status for the multi-chassis ipsec peer *$tmnxMcPeerIpAddr $* tunnel-group *$tMcPeerIPsecTnlGrpId$* changed to *$tMcPeerIPsecTnl GrpProtectStatus$*
Cause	The notification tMcPeerIPsecTnlGrpProtStatusChg is generated whenever protection status of a tunnel-group changes.
Effect	This notification is informational. A change in tMcPeerIPsecTnlGrp ProtectStatus to 'nominal' indicates protection status readiness for switchover.
Recovery	No recovery actions are required.

38.4 tmnxMCEPSessionPsvModeDisabled

Table 686: tmnxMCEPSessionPsvModeDisabled properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2034
Event name	tmnxMCEPSessionPsvModeDisabled
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.33
Default severity	warning
Message format string	Passive-mode for the multi-chassis endpoint peer *$tmnxMcPeerIpAddr $* with source *$tmnxMcPeerSrcIpAddr$* is disabled
Cause	Passive-mode for the session between a multi-chassis endpoint and its peer has been 'disabled' from either local or peer.
Effect	N/A
Recovery	Configure passive-mode enabled on local or peer multi-chassis endpoint.

38.5 tmnxMCEPSessionPsvModeEnabled

Table 687: tmnxMCEPSessionPsvModeEnabled properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2033
Event name	tmnxMCEPSessionPsvModeEnabled
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.32
Default severity	warning
Message format string	Passive-mode for the multi-chassis endpoint peer *$tmnxMcPeerIpAddr $* with source *$tmnxMcPeerSrcIpAddr$* is enabled. Passive-mode with peer has *$tmnxMcPeerEPPsvModeConfigState$*

Property name	Value
Cause	Passive-mode for the session between a multi-chassis endpoint and its peer has been 'enabled' from either local or peer.
Effect	N/A
Recovery	N/A

38.6 tmnxMcLagInfoLagChanged

Table 688: tmnxMcLagInfoLagChanged properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2014
Event name	tmnxMcLagInfoLagChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.14
Default severity	warning
Message format string	tmnxMcLagInfoLagTable: Peer *$tmnxMcPeerIpAddrForNotify$* configuration changed.
Cause	Entries in tmnxMcLagInfoLagTable were changed.
Effect	N/A
Recovery	No recovery is necessary.

38.7 tmnxMcOmcrClientNumEntriesHigh

Table 689: tmnxMcOmcrClientNumEntriesHigh properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2038
Event name	tmnxMcOmcrClientNumEntriesHigh
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.38

Property name	Value
Default severity	minor
Message format string	The number of warm standby MCS entries for application *$tmnxMcs ClientApplication$* is becoming too high: *$tmnxMcNotifyNumber$*% (peer *$tmnxMcPeerIpAddr$*)
Cause	The notification tmnxMcOmcrClientNumEntriesHigh is generated when the this system is configured as an OMCR warm standby system, and the total number of entries in the MCS database for a particular application becomes high. This system is configured as a warm standby system as soon as the value of the object tmnxMcPeerWarm Standby is equal to 'true' for any multi-chassis peer in this system. The total number of entries is the sum of the values of the object tmnxMcs ClientNumEntries for the client application specified by tmnxMcsClient Application. The maximum number of entries for a client application is equal to one million. The value of tmnxMcNotifyNumber indicates the ratio in percent of the total number of entries and the maximum number of entries. The threshold ratios are at 80%, 90% and 100%. The values of tmnxMcPeerIpType and tmnxMcPeerIpAddr indicate the peer that reached the treshold.
Effect	When the 80% and 90% threshold is crossed, there is no effect. When the 100% threshold is exceeded, the peer indicated by the values of tmnxMcPeerIpType and tmnxMcPeerIpAddr is shut down automatically by this system (the value of tmnxMcPeerSyncAdminState is set to 'out OfService' and the value of tmnxMcPeerSyncOperFlags is set to 'omcr NumEntriesHigh').
Recovery	Reconfigure the oversubscribed multi-chassis redundancy set-up to reduce the number of entries protected by this system. When the total number of entries in the MCS database for this client application becomes lower than the 80% threshold again, there is no further notification.

38.8 tmnxMcOmcrStatFailedChanged

Table 690: tmnxMcOmcrStatFailedChanged properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2037
Event name	tmnxMcOmcrStatFailedChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.37

Property name	Value
Default severity	minor
Message format string	*$tmnxMcOmcrStatClientApplication$* OMCR protection with *$tmnx McOmcrStatAccessProtection$* instance *$tmnxMcOmcrStatIndex$ $tmnxMcOmcrStatFailed$ - $tmnxMcOmcrStatFailure$*
Cause	The notification tmnxMcOmcrStatFailedChanged is generated the value of the object tmnxMcOmcrStatFailed changes. The most interesting change is from 'nA' to any of the other values; when an OMCR client application access protection instance (for example an SRRP instance) becomes active, the system will attempt to allocate resources for all associated client application entries (for example IPOE subscriber hosts); if this succeeds, the value of tmnxMcOmcrStatFailed becomes 'no', if it fails, it becomes 'yes'.
Effect	TODO.
Recovery	TODO.

38.9 tmnxMcPeerEPBfdSessionClose

Table 691: tmnxMcPeerEPBfdSessionClose properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2028
Event name	tmnxMcPeerEPBfdSessionClose
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.27
Default severity	warning
Message format string	Multi-Chassis endpoint closed BFD session for peer *$tmnxMcPeer IpAddr$* with source *$tmnxMcPeerSrcIpAddr$*
Cause	A multi-chassis endpoint is closing a BFD session to the multi-chassis endpoint peer.
Effect	N/A
Recovery	N/A

38.10 tmnxMcPeerEPBfdSessionDown

Table 692: tmnxMcPeerEPBfdSessionDown properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2030
Event name	tmnxMcPeerEPBfdSessionDown
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.29
Default severity	warning
Message format string	Operational state of the BFD session for multi-chassis endpoint peer *$tmnxMcPeerIpAddr$* and source *$tmnxMcPeerSrcIpAddr$* is changed to down
Cause	The operational state of a BFD session between a multi-chassis endpoint and its peer has changed to 'down'.
Effect	N/A
Recovery	N/A

38.11 tmnxMcPeerEPBfdSessionOpen

Table 693: tmnxMcPeerEPBfdSessionOpen properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2027
Event name	tmnxMcPeerEPBfdSessionOpen
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.26
Default severity	warning
Message format string	Multi-Chassis endpoint attempted to open BFD session for peer *$tmnx McPeerIpAddr$* and source *$tmnxMcPeerSrcIpAddr$* with status= *$tmnxMcPeerEPBfdSessionOpenStatus$*
Cause	A multi-chassis endpoint is attempting to open a BFD session to the mutli-chassis endpoint peer.

Property name	Value
Effect	N/A
Recovery	N/A

38.12 tmnxMcPeerEPBfdSessionUp

Table 694: tmnxMcPeerEPBfdSessionUp properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2029
Event name	tmnxMcPeerEPBfdSessionUp
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.28
Default severity	warning
Message format string	Operational state of the BFD session for multi-chassis endpoint peer *$tmnxMcPeerIpAddr$* and source *$tmnxMcPeerSrcIpAddr$* is changed to up
Cause	The operational state of a BFD session between a multi-chassis endpoint and its peer is changed to 'up'.
Effect	N/A
Recovery	N/A

38.13 tmnxMcPeerEPOperDown

Table 695: tmnxMcPeerEPOperDown properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2031
Event name	tmnxMcPeerEPOperDown
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.30

Property name	Value
Default severity	warning
Message format string	Multi-Chassis endpoint peer *$tmnxMcPeerIpAddr$* with source *$tmnx McPeerSrcIpAddr$* oper state changed to Down
Cause	A multi-chassis endpoint detected a time-out while communicating with the multi-chassis endpoint peer.
Effect	N/A
Recovery	N/A

38.14 tmnxMcPeerEPOperUp

Table 696: tmnxMcPeerEPOperUp properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2032
Event name	tmnxMcPeerEPOperUp
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.31
Default severity	warning
Message format string	Multi-Chassis endpoint peer *$tmnxMcPeerSrcIpAddr$* with source *$tmnxMcPeerIpAddr$* oper state changed to Up
Cause	A multi-chassis endpoint has cleared the time-out condition in communicating with the multi-chassis endpoint peer.
Effect	N/A
Recovery	N/A

38.15 tmnxMcPeerRingsOperStateChanged

Table 697: tmnxMcPeerRingsOperStateChanged properties

Property name	Value
Application name	MC_REDUNDANCY

Property name	Value
Event ID	2022
Event name	tmnxMcPeerRingsOperStateChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.16
Default severity	warning
Message format string	The MC-Ring operational state of peer *$tmnxMcPeerIpAddr$* changed to *$tmnxMcPeerRingsOperState$*.
Cause	The operational state, with respect to multi-chassis ring operation, of a peer changed. state | cause ---------- unknown | No rings are configured for this peer. inService | The signalling connection for mc-ring operation | is operational. out OfService | The signalling connection for mc-ring operation | has timed out. transition | Not implemented.
Effect	state | effect ---------- unknown | None. inService | The signalling connection for mc-ring operation | is operational. outOfService | None, as long as no rings are in state 'broken'. | The MCS connection is likely to be out of service. | If some rings are in state 'broken', those rings | will suffer degraded functionality. transition | Not implemented.
Recovery	The recovery depends on the operational state of the ring: state | recovery ---------- unknown | None. inService | None. outOfService | Restore the IP connectivity between the local peer | and the remote peer. transition | Not implemented.

38.16 tmnxMcPeerSyncStatusChanged

Table 698: tmnxMcPeerSyncStatusChanged properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2004
Event name	tmnxMcPeerSyncStatusChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.4
Default severity	warning

Property name	Value
Message format string	The Sync status of peer *$tmnxMcPeerIpAddr$* changed to *$tmnx McPeerSyncStatus$*
Cause	The event is generated when the sync state changes.
Effect	N/A
Recovery	No recovery is necessary.

38.17 tmnxMcRedundancyMismatchDetected

Table 699: tmnxMcRedundancyMismatchDetected properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2002
Event name	tmnxMcRedundancyMismatchDetected
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.2
Default severity	warning
Message format string	*$tmnxMcLagConfigMismatchString$*
Cause	The event is generated when a configuration mismatch is detected.
Effect	N/A
Recovery	No recovery is necessary.

38.18 tmnxMcRedundancyMismatchResolved

Table 700: tmnxMcRedundancyMismatchResolved properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2003
Event name	tmnxMcRedundancyMismatchResolved
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.3

Property name	Value
Default severity	warning
Message format string	*$tmnxMcLagConfigMismatchString$*
Cause	The event is generated when a configuration mismatch is resolved.
Effect	N/A
Recovery	No recovery is necessary.

38.19 tmnxMcRedundancyPeerStateChanged

Table 701: tmnxMcRedundancyPeerStateChanged properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2001
Event name	tmnxMcRedundancyPeerStateChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.1
Default severity	warning
Message format string	The MC-LAG operational status of peer *$tmnxMcPeerIpAddr$* changed to *$tmnxMcLagConfigOperState$*
Cause	The event is generated when the a MC lag has changed its operational state.
Effect	N/A
Recovery	No recovery is necessary.

38.20 tmnxMcRingInbCtrlOperStateChgd

Table 702: tmnxMcRingInbCtrlOperStateChgd properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2017
Event name	tmnxMcRingInbCtrlOperStateChgd

Property name	Value
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.17
Default severity	warning
Message format string	The MC-Ring operational state of the inband control connection of ring *$tmnxMcPeerIpAddr$*::*$tmnxMcPeerSyncPortSyncTag$* changed to *$tmnxMcRingInfoOperState$*.
Cause	The event is generated when when the operational state of a multi-chassis ring's inband control connection changes. state | cause ---------- unknown connected : the inband control connection with the peer is operational; broken : the inband control connection with the peer has timed out; testing : the inband control connection with the peer is being set up. Waiting for result. notConfigured : the inband control connection with the peer is not configured."
Effect	The operational state of the inband control connection affects the operational state of the ring.
Recovery	The recovery depends on the operational state of the ring.

38.21 tmnxMcRingNodeLocOperStateChgd

Table 703: tmnxMcRingNodeLocOperStateChgd properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2018
Event name	tmnxMcRingNodeLocOperStateChgd
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.18
Default severity	warning
Message format string	The MC-Ring Node operational state of ring node *$tmnxMcPeer IpAddr$*::*$tmnxMcPeerSyncPortSyncTag$*::*$tmnxMcRingNodeName $* changed to *$tmnxMcRingNodeInfoLocOperState$* while in-use is *$tmnxMcRingNodeInfoInUse$*.
Cause	The event is generated when when the operational state of a multi-chassis ring's inband control connection changes. state | cause ---------- unknown : notProvisioned: the node is configured on the peer but not on this system; configErr :

Property name	Value
	the local configuration of the node is incorrect notTested : the ring node connectivity verification is shut down; testing : temporary state; connected : disconnected :
Effect	state | effect ---------- unknown : notProvisioned: no effect; configErr : no effect; notTested : no effect; testing : no effect; the effect of the operational state of the ring node depends on the operational state of the ring; only when the operational state of the ring is 'broken', ... connected : ... all MAC addresses associated with this ring node are put on the SAP; disconnected : ... all MAC addresses associated with this ring node are put on the shunt;
Recovery	Recovery is only required if the operational state of the ring is 'broken'. Repair the ring connection with the peer.

38.22 tmnxMcRingOperStateChanged

Table 704: tmnxMcRingOperStateChanged properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2016
Event name	tmnxMcRingOperStateChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.16
Default severity	warning
Message format string	The MC-Ring operational state of ring *$tmnxMcPeerIpAddr$*::*$tmnx McPeerSyncPortSyncTag$* changed to *$tmnxMcRingInfoOperState$*.
Cause	The event is generated when the operational state of the MC-Ring has changed. state | cause ---------- unknown shutdown configErr noPeer : the peer has no corresponding ring configured; connected : the inband control connection with the peer is operational; broken : the inband control connection with the peer has timed out; localBroken : the inband control connection with the peer is known to be broken because of a local failure or local administrative action; conflict : the inband control connection with the peer has timed out but the physical connection is still OK; the failure of the inband signaling connection is caused by some misconfiguration. E.g. a conflict between the configuration of this system and its peer, or a misconfiguration on one of the ring access node systems. testing Ring : the inband control connection with the peer is being set up.

Property name	Value
	Waiting for result. waitingForPeer: verifying if this ring is configured on the peer.
Effect	state | effect ---------- unknown shutdown : the ring brings all SAP's of path-a and path-b in operational state 'up'. configErr : if there is no peer ring, the ring brings all SAP's on path-a and path-b in operational state 'up'; if there is a peer ring, the ring brings all SAP's on path-a and path-b in operational state 'down'. noPeer : the ring brings all SAP's of path-a and path-b in operational state 'up'. connected : the ring brings all SAP's of its own path in operational state 'up' and all SAP's of the other path in operational state 'down'. broken : the ring brings all SAP's of path-a and path-b in operational state 'up'. localBroken : this system brings all SAP's of path-a and path-b in operational state 'down' unless they belong to the excluded-path. conflict : the ring brings all SAP's of its own path in operational state 'up' and all SAP's of the other path in operational state 'down'. testingRing : the ring does not change the operational state of any SAP. waitingForPeer: the ring does not change the operational state of any SAP.
Recovery	The recovery depends on the operational state of the ring: state | recovery ---------- unknown shutdown : no recovery required. configErr : correct the configuration of the ring on this system. noPeer : no recovery required. connected : no recovery required. broken : repair the ring connection with the peer. localBroken : repair the local failure or undo the administrative action that caused the failure. conflict : make the ring configuration on this system consistent with the ring configuration on the peer. testingRing : temporary state. waitingForPeer: temporary state.

38.23 tmnxMcSyncClientAlarmCleared

Table 705: tmnxMcSyncClientAlarmCleared properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2006
Event name	tmnxMcSyncClientAlarmCleared
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.6
Default severity	warning
Message format string	*$tmnxMcPeerSyncClient$* back in sync with peer *$tmnxMcPeerIpAddrForNotify$*.

Property name	Value
Cause	The event is generated when the application has the resources to become in sync again.
Effect	N/A
Recovery	No recovery is necessary.

38.24 tmnxMcSyncClientAlarmRaised

Table 706: tmnxMcSyncClientAlarmRaised properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2005
Event name	tmnxMcSyncClientAlarmRaised
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.5
Default severity	warning
Message format string	*$tmnxMcPeerSyncClient$* lost sync with peer *$tmnxMcPeerIpAddrForNotify$*.
Cause	The event is generated when the application runs out of resources to sync with the database.
Effect	N/A
Recovery	No recovery is necessary.

38.25 tmnxMcSyncClockSkewCleared

Table 707: tmnxMcSyncClockSkewCleared properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2020
Event name	tmnxMcSyncClockSkewCleared
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.20

Property name	Value
Default severity	warning
Message format string	The system clock for MCS peer *$tmnxMcPeerIpAddrForNotify$* differs *$tmnxMcPeerClockSkew$* seconds from the local system clock.
Cause	The MCS peer system clock time has returned to less than 60 seconds different than the local system clock. This notification would only be generated following a tmnxMcSyncClockSkewRaised notification.
Effect	N/A
Recovery	No recovery is necessary.

38.26 tmnxMcSyncClockSkewRaised

Table 708: tmnxMcSyncClockSkewRaised properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2019
Event name	tmnxMcSyncClockSkewRaised
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.19
Default severity	warning
Message format string	The system clock for MCS peer *$tmnxMcPeerIpAddrForNotify$* differs *$tmnxMcPeerClockSkew$* seconds from the local system clock.
Cause	The MCS peer system clock time is greater than 60 seconds different than the local system clock.
Effect	N/A
Recovery	No recovery is necessary.

38.27 tmnxSrrpBecameBackup

Table 709: tmnxSrrpBecameBackup properties

Property name	Value
Application name	MC_REDUNDANCY

Property name	Value
Event ID	2024
Event name	tmnxSrrpBecameBackup
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.24
Default severity	minor
Message format string	SRRP instance *$tmnxSrrpOperID$* on interface *$vRtrIfIndex$* changed state to backup - current master is *$tmnxMcPeerIpAddrForNotify$*
Cause	The sending agent has transitioned to 'Backup' state.
Effect	N/A
Recovery	N/A

38.28 tmnxSrrpBfdIntfSessStateChgd

Table 710: tmnxSrrpBfdIntfSessStateChgd properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2026
Event name	tmnxSrrpBfdIntfSessStateChgd
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.25
Default severity	minor
Message format string	BFD session on service *$tmnxSrrpNotifBfdIntfSvcId$* interface *$tmnx SrrpNotifBfdIntfIfName$* to peer *$tmnxSrrpNotifBfdIntfDestIp$* changed state to *$tmnxSrrpNotifBfdIntfSessState$*.
Cause	The operational state of BFD session of the SRRP instance changed.
Effect	N/A
Recovery	N/A

38.29 tmnxSrrpDualMaster

Table 711: tmnxSrrpDualMaster properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2013
Event name	tmnxSrrpDualMaster
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.13
Default severity	warning
Message format string	SRRP ID *$tmnxSrrpOperID$*: Dual Master detected on both peer *$tmnxMcPeerIpAddrForNotify$* / interface *$tmnxMcRemoteGrpIfName ForNotify$* and local *$tmnxMcPeerSrcIpAddr$* / interface *$vRtrIfIndex$*.
Cause	Both the local and remote SRRP instances are in the master state.
Effect	N/A
Recovery	No recovery is necessary.

38.30 tmnxSrrpDuplicateSubIfAddress

Table 712: tmnxSrrpDuplicateSubIfAddress properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2021
Event name	tmnxSrrpDuplicateSubIfAddress
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.21
Default severity	warning
Message format string	SRRP id *$tmnxSrrpOperID$*: IP Address on interface *$vRtrIfIndex$* on local node *$tmnxMcPeerSrcIpAddr$* conflicts with IP Address on node *$tmnxMcPeerIpAddrForNotify$*.
Cause	The IP address for a local subscriber interface conflicts with the IP address for a remote subscriber interface.
Effect	N/A

Property name	Value
Recovery	Resolve IP address conflict.

38.31 tmnxSrrpInstanceIdMismatch

Table 713: tmnxSrrpInstanceIdMismatch properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2009
Event name	tmnxSrrpInstanceIdMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.9
Default severity	warning
Message format string	The SRRP Id from node *$tmnxMcPeerIpAddrForNotify$* did not match srrp *$tmnxSrrpOperID$* on local node *$tmnxMcPeerSrcIpAddr$*: interface *$vRtrIfIndex$*.
Cause	The notification tmnxSrrpInstanceIdMismatch is generated when an SRRP instance has detected that at least one SAP it is protecting is associated with a different SRRP instance on the remote peer.
Effect	One or more SAPs are not protected by SRRP.
Recovery	Verify configuration on the local and remote end routers to ensure that all SAPs are associated with the same SRRP instance on both sides.

38.32 tmnxSrrpOperDownInvalidMac

Table 714: tmnxSrrpOperDownInvalidMac properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2043
Event name	tmnxSrrpOperDownInvalidMac
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.39
Default severity	minor

Property name	Value
Message format string	tmnxSrrpOperDownInvalidMac notification from SRRP id *$tmnxSrrp OperID$* on interface *$vRtrIfIndex$*. SRRP instance is not allowed to be operational.
Cause	tmnxSrrpOperDownInvalidMac is generated when the operational virtual MAC of an SRRP instance conflicts with the MAC of the parent interface.
Effect	The SRRP virtual router instance is not allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification.

38.33 tmnxSrrpOperDownInvalidMacClear

Table 715: tmnxSrrpOperDownInvalidMacClear properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2044
Event name	tmnxSrrpOperDownInvalidMacClear
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.40
Default severity	minor
Message format string	tmnxSrrpOperDownInvalidMac notification from SRRP id *$tmnxSrrp OperID$* on interface *$vRtrIfIndex$* has been cleared.
Cause	The tmnxSrrpOperDownInvalidMacClear is generated when a previously occurring tmnxSrrpOperDownInvalidMac notification has been cleared. Operational virtual MAC of an IPv4 SRRP instance does not have any conflict with the MAC of the parent interface.
Effect	The SRRP virtual router instance is allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification."

38.34 tmnxSrrpRedIfMismatch

Table 716: tmnxSrrpRedIfMismatch properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2012
Event name	tmnxSrrpRedIfMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.12
Default severity	warning
Message format string	SRRP ID *$tmnxSrrpOperID$*: Redundant interface *$tmnxMcRemote RedIfNameForNotify$* on peer *$tmnxMcPeerIpAddrForNotify$* / interface *$tmnxMcRemoteGrpIfNameForNotify$* does not match local *$tmnxMcPeerSrcIpAddr$* / interface *$vRtrIfIndex$*.
Cause	The local and remote redundant interfaces are not properly paired.
Effect	N/A
Recovery	No recovery is necessary.

38.35 tmnxSrrpSapMismatch

Table 717: tmnxSrrpSapMismatch properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2010
Event name	tmnxSrrpSapMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.10
Default severity	warning
Message format string	SRRP id *$tmnxSrrpOperID$*: SAPs on peer interface *$tmnxMcRemote GrpIfNameForNotify$* do not match those on local interface *$vRtr IfIndex$*.
Cause	The SAPs SRRP is backing up on the local interface do not match with the ones on the remote interface.

Property name	Value
Effect	N/A
Recovery	No recovery is necessary.

38.36 tmnxSrrpSapTagMismatch

Table 718: tmnxSrrpSapTagMismatch properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2011
Event name	tmnxSrrpSapTagMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.11
Default severity	warning
Message format string	SRRP ID *$tmnxSrrpOperID$*: SAP encap of *$sapEncapValue$* on peer interface *$tmnxMcRemoteGrpIfNameForNotify$* has MCS tag *$tmnx McRemoteSyncTag$*, which differs from local tag *$tmnxMcPeerSync PortEncapSyncTag$* on interface *$vRtrIfIndex$*.
Cause	The tag for a local SAP does not match those of the remote SAP.
Effect	N/A
Recovery	No recovery is necessary.

38.37 tmnxSrrpSubnetMismatch

Table 719: tmnxSrrpSubnetMismatch properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2007
Event name	tmnxSrrpSubnetMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.7
Default severity	warning

Property name	Value
Message format string	IP Address list from node *$tmnxMcPeerIpAddrForNotify$* did not match the address list configured for SRRP instance *$tmnxSrrpOperID$* on local node *$tmnxMcPeerSrcIpAddr$*: interface *$vRtrIfIndex$*.
Cause	The IP address list received through SRRP-MCS synchronization received from the current master does not match the local configured IP address list.
Effect	This is an edge triggered notification. A second trap will not be generated for a packet from the same master until this event has been cleared.
Recovery	No recovery is necessary.

38.38 tmnxSrrpSubnetMismatchCleared

Table 720: tmnxSrrpSubnetMismatchCleared properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2008
Event name	tmnxSrrpSubnetMismatchCleared
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.8
Default severity	warning
Message format string	IP Address list from node *$tmnxMcPeerIpAddrForNotify$* matched the address list configured for SRRP instance *$tmnxSrrpOperID$* on local node *$tmnxMcPeerSrcIpAddr$*: interface *$vRtrIfIndex$*.
Cause	The mismatch in the IP address list received through SRRP-MCS synchronization received from the current master is cleared.
Effect	N/A
Recovery	No recovery is necessary.

38.39 tmnxSrrpSystemIpNotSet

Table 721: tmnxSrrpSystemIpNotSet properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2015
Event name	tmnxSrrpSystemIpNotSet
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.15
Default severity	warning
Message format string	SRRP sending out advertisement packets before the system IP address has been set.
Cause	SRRP tried to send out advertisement packets but the system IP address is not set.
Effect	SRRP sends out advertisement packets with a source address of 0.0.0.0.
Recovery	No recovery is necessary.

38.40 tmnxSrrpTrapNewMaster

Table 722: tmnxSrrpTrapNewMaster properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2023
Event name	tmnxSrrpTrapNewMaster
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.23
Default severity	minor
Message format string	SRRP instance *$tmnxSrrpOperID$* on interface *$vRtrIfIndex$* (primary address *$tmnxMcPeerIpAddrForNotify$*) changed state to master
Cause	The sending multi-chassis SRRP instance has transitioned to 'Master' state.
Effect	N/A

Property name	Value
Recovery	N/A

39 MCPATH

39.1 tmnxMcPathAvailBwLimitReached

Table 723: tmnxMcPathAvailBwLimitReached properties

Property name	Value
Application name	MCPATH
Event ID	2003
Event name	tmnxMcPathAvailBwLimitReached
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.3
Default severity	minor
Message format string	The available bandwidth on *$strTmnxMcPathChlPathType$* path on slot/cplx *$tmnxMcPathCardSlotNum$*/ *$tmnxMcPathMDASlotNum$* has reached its maximum limit.
Cause	The available bandwidth limit has been reached.
Effect	N/A
Recovery	N/A

39.2 tmnxMcPathAvailBwValWithinRange

Table 724: tmnxMcPathAvailBwValWithinRange properties

Property name	Value
Application name	MCPATH
Event ID	2004
Event name	tmnxMcPathAvailBwValWithinRange
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.4
Default severity	minor

Property name	Value
Message format string	The available bandwidth on *$strTmnxMcPathChlPathType$* path on slot/cplx *$tmnxMcPathCardSlotNum$*/ *$tmnxMcPathMDASlotNum$* is within range limits.
Cause	The available bandwidth limit fell below the maximum limit and is within the permitted range.
Effect	N/A
Recovery	N/A

39.3 tmnxMcPathSrcGrpBlkHole

Table 725: tmnxMcPathSrcGrpBlkHole properties

Property name	Value
Application name	MCPATH
Event ID	2001
Event name	tmnxMcPathSrcGrpBlkHole
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.1
Default severity	minor
Message format string	Channel (*$tmnxMcPathChlSrcAddr$*, *$tmnxMcPathChlGrpAddr$*) for *$tmnxMcPathChlRtrType$* instance *$vRtrID$* slot/cplx *$tmnxMcPath CardSlotNum$*/*$tmnxMcPathMDASlotNum$* has been blackholed.
Cause	A source group(S,G) went into a black-hole state."
Effect	N/A
Recovery	N/A

39.4 tmnxMcPathSrcGrpBlkHoleClear

Table 726: tmnxMcPathSrcGrpBlkHoleClear properties

Property name	Value
Application name	MCPATH
Event ID	2002

Property name	Value
Event name	tmnxMcPathSrcGrpBlkHoleClear
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.2
Default severity	minor
Message format string	Channel (*$tmnxMcPathChlSrcAddr$*, *$tmnxMcPathChlGrpAddr$*) for *$vRtrType$* instance *$vRtrID$* slot/cplx *$tmnxMcPathCardSlotNum$*/*$tmnxMcPathMDASlotNum$* is no longer being blackholed.
Cause	A source, group(S,G), went out of the black-hole state.
Effect	N/A
Recovery	N/A

40 MIRROR

40.1 destinationDisabled

Table 727: destinationDisabled properties

Property name	Value
Application name	MIRROR
Event ID	2004
Event name	destinationDisabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.4
Default severity	minor
Message format string	Mirror destination *$tMirrorDestinationIndex$* is administratively disabled ('shutdown')
Cause	The operator disabled the mirror destination.
Effect	No mirror traffic will egress. Applications using the mirror traffic will not receive any traffic from this destination.
Recovery	The operator intentionally disabled the mirror destination, so no recovery is necessary. Enable the mirror destination to restart mirroring.

40.2 destinationEnabled

Table 728: destinationEnabled properties

Property name	Value
Application name	MIRROR
Event ID	2003
Event name	destinationEnabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.3
Default severity	minor

Property name	Value
Message format string	Mirror destination *$tMirrorDestinationIndex$* is administratively enabled ('no shutdown')
Cause	The operator enabled the mirror destination.
Effect	Mirror traffic will egress. Applications using the mirror traffic will receive traffic from this destination.
Recovery	The operator intentionally enabled the mirror destination, so no recovery is necessary.

40.3 sourceDisabled

Table 729: sourceDisabled properties

Property name	Value
Application name	MIRROR
Event ID	2002
Event name	sourceDisabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.2
Default severity	minor
Message format string	Mirror source *$tMirrorSourceIndex$* is administratively disabled ('shutdown')
Cause	The operator disabled the mirror source.
Effect	No traffic from this source will be mirrored. Applications using the mirror traffic will not receive any traffic from this source.
Recovery	The operator intentionally disabled the mirror source, so no recovery is required. Enable the mirror source to restart mirroring.

40.4 sourceEnabled

Table 730: sourceEnabled properties

Property name	Value
Application name	MIRROR
Event ID	2001

Property name	Value
Event name	sourceEnabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.1
Default severity	minor
Message format string	Mirror source *$tMirrorSourceIndex$* is administratively enabled ('no shutdown')
Cause	The operator enabled the mirror source.
Effect	Traffic from this source will be mirrored. Applications using the mirror traffic will receive traffic from this source.
Recovery	The operator intentionally enabled the mirror source, so no recovery is required. Disable the mirror source to stop mirroring.

40.5 sourceIpFilterChange

Table 731: sourceIpFilterChange properties

Property name	Value
Application name	MIRROR
Event ID	2006
Event name	sourceIpFilterChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.6
Default severity	minor
Message format string	Mirror source *$tMirrorSourceIndex$* associated IP filter *$tMirrorSourceFilterId$* entry *$tMirrorSourceFilterEntryId$* has been *$tMirrorSourceChangeType$*
Cause	An IP filter or filter entry associated with the mirror source has been modified or deleted.
Effect	Mirrored traffic from this source may be affected in an undesired manner.
Recovery	Modify the configuration of the associated IP filter or filter entry to restore the desired mirrored traffic.

40.6 sourceMacFilterChange

Table 732: sourceMacFilterChange properties

Property name	Value
Application name	MIRROR
Event ID	2007
Event name	sourceMacFilterChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.7
Default severity	minor
Message format string	Mirror source *$tMirrorSourceIndex$* associated MAC filter *$tMirror SourceFilterId$* entry *$tMirrorSourceFilterEntryId$* has been *$tMirror SourceChangeType$*
Cause	A MAC filter or filter entry associated with the mirror source has been modified or deleted.
Effect	Mirrored traffic from this source may be affected in an undesired manner.
Recovery	Modify the configuration of the associated MAC filter or filter entry to restore the desired mirrored traffic.

40.7 sourceSapChange

Table 733: sourceSapChange properties

Property name	Value
Application name	MIRROR
Event ID	2008
Event name	sourceSapChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.8
Default severity	minor
Message format string	Mirror source *$tMirrorSourceIndex$* associated SAP *$tMirrorSource SapEncapValue$* has been *$tMirrorSourceChangeType$*
Cause	A SAP associated with the mirror source has been modified or deleted.
Effect	Mirrored traffic from this source may be affected in an undesired manner.

Property name	Value
Recovery	Modify the configuration of the associated SAP to restore the desired mirrored traffic.

40.8 sourceSubscriberChange

Table 734: sourceSubscriberChange properties

Property name	Value
Application name	MIRROR
Event ID	2009
Event name	sourceSubscriberChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.9
Default severity	minor
Message format string	Mirror source *$tMirrorSourceIndex$* associated subscriber "*$tMirror SourceSubIdent$*" has been *$tMirrorSourceChangeType$*
Cause	A subscriber associated with the mirror source has been activated, deactivated, modified or deleted.
Effect	Mirrored traffic from this source may be affected in an undesired manner.
Recovery	Modify the configuration of the associated subscriber to restore the desired mirrored traffic.

40.9 tMirrorSourceIpv6FilterChange

Table 735: tMirrorSourceIpv6FilterChange properties

Property name	Value
Application name	MIRROR
Event ID	2022
Event name	tMirrorSourceIpv6FilterChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.22
Default severity	minor

Property name	Value
Message format string	Mirror source *$tMirrorSourceIndex$* associated IPv6 filter *$tMirror SourceFilterId$* entry *$tMirrorSourceFilterEntryId$* has been *$tMirror SourceChangeType$*
Cause	The tMirrorSourceIpv6FilterChange event is generated when a IPv6 filter or filter entry associated with the mirror-source indicated by t MirrorSourceIndex is 'modified' or 'deleted'. If the only the base filter is modified, tMirrorSourceFilterEntryId will have a value of 0.
Effect	Mirrored traffic from this source may be affected in an undesired manner.
Recovery	Modify the configuration of the associated IP filter or filter entry to restore the desired mirrored traffic.

41 MLD

41.1 vRtrMldGrpIfSapCModeRxQueryMism

Table 736: vRtrMldGrpIfSapCModeRxQueryMism properties

Property name	Value
Application name	MLD
Event ID	2015
Event name	vRtrMldGrpIfSapCModeRxQueryMism
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.15
Default severity	warning
Message format string	Compatible mode oper version *$vRtrMldGrpIfSapOperVersion$* mismatches query version *$vRtrMldNotifyQueryVersion$*
Cause	A vRtrMldGrpIfSapCModeRxQueryMism notification is generated when there is a mismatch between the compatible mode of the MLD SAP and the version of the received query. It is generated when the SAP is in MLDv1 compatible mode but it receives an MLDv2. sapPortId and sapEncapValue will identify the SAP on which the query is received. vRtrMldGrpIfSapOperVersion will indicate the compatibility mode of the SAP and vRtrMldNotifyQueryVersion will contain the version of the received query.
Effect	N/A
Recovery	N/A

41.2 vRtrMldGrpIfSapMaxGrpsLimExceed

Table 737: vRtrMldGrpIfSapMaxGrpsLimExceed properties

Property name	Value
Application name	MLD
Event ID	2012
Event name	vRtrMldGrpIfSapMaxGrpsLimExceed

Property name	Value
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.12
Default severity	warning
Message format string	Number of groups exceeds *$vRtrMldGrpIfSapMaxGroups$* on SAP
Cause	The vRtrMldGrpIfSapMaxGrpsLimExceed event is generated when an attempt is made to configure a group when vRtrMldGrpIfSapGroup Count, the number of groups configured on the SAP, is equal to vRtr MldGrpIfSapMaxGroups, the maximum number of groups supported on the SAP.
Effect	N/A
Recovery	N/A

41.3 vRtrMldGrpIfSapMaxGrpSrcLimExcd

Table 738: vRtrMldGrpIfSapMaxGrpSrcLimExcd properties

Property name	Value
Application name	MLD
Event ID	2019
Event name	vRtrMldGrpIfSapMaxGrpSrcLimExcd
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.19
Default severity	warning
Message format string	Max group sources exceeded *$vRtrMldGrpIfSapMaxGrpSources$* for SAP
Cause	The vRtrMldGrpIfSapMaxGrpSrcLimExcd event is generated when an attempt is made to configure a group source for a group when the number of group sources is equal to vRtrMldGrpIfSapMaxGrpSources, the maximum number of group sources per group supported on the SAP.
Effect	N/A
Recovery	N/A

41.4 vRtrMldGrpIfSapMaxSrcsLimExceed

Table 739: vRtrMldGrpIfSapMaxSrcsLimExceed properties

Property name	Value
Application name	MLD
Event ID	2013
Event name	vRtrMldGrpIfSapMaxSrcsLimExceed
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.13
Default severity	warning
Message format string	Max number of source per group exceeded *$vRtrMldGrpIfSapMax Sources$* for SAP
Cause	The vRtrMldGrpIfSapMaxSrcsLimExceed event is generated when an attempt is made to configure a source for a group when the number of sources for this group is equal to vRtrMldGrpIfSapMaxSources, the maximum number of sources per group supported on the SAP.
Effect	N/A
Recovery	N/A

41.5 vRtrMldGrpIfSapMcacPlcyDropped

Table 740: vRtrMldGrpIfSapMcacPlcyDropped properties

Property name	Value
Application name	MLD
Event ID	2014
Event name	vRtrMldGrpIfSapMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.14
Default severity	warning
Message format string	MLD group *$vRtrMldNotifyGrpAddr$* dropped because applying plcy *$vRtrMldNotifyMcacPolicyName$*
Cause	The vRtrMldGrpIfSapMcacPlcyDropped event is generated when an MLD group is dropped on a given SAP because of applying a multicast CAC policy given by vRtrMldNotifyMcacPolicyName.
Effect	N/A

Property name	Value
Recovery	N/A

41.6 vRtrMldGrpIfSapRxQueryVerMism

Table 741: vRtrMldGrpIfSapRxQueryVerMism properties

Property name	Value
Application name	MLD
Event ID	2016
Event name	vRtrMldGrpIfSapRxQueryVerMism
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.16
Default severity	warning
Message format string	SAP configured for MLDv *$vRtrMldGrpIfSapAdminVersion$* received MLDv*$vRtrMldNotifyQueryVersion$* query
Cause	A vRtrMldGrpIfSapRxQueryVerMism notification is generated when the MLD host SAP is configured as MLDv2 but receives an MLDv1 Query. sapPortId and sapEncapValue will identify the SAP on which the query is received. vRtrMldGrpIfSapAdminVersion will contain the configured version of the SAP and vRtrMldNotifyQueryVersion will contain the version of the received query.
Effect	N/A
Recovery	N/A

41.7 vRtrMldHostCModeRxQueryMismatch

Table 742: vRtrMldHostCModeRxQueryMismatch properties

Property name	Value
Application name	MLD
Event ID	2008
Event name	vRtrMldHostCModeRxQueryMismatch
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.8
Default severity	warning

Property name	Value
Message format string	Mismatch between oper version *$vRtrMldHostOperVersion$* and query version *$vRtrMldNotifyQueryVersion$*
Cause	A vRtrMldHostCModeRxQueryMismatch notification is generated when there is a mismatch between the compatible mode of the MLD Host and the version of the received query. It is generated when the Host is in MLDv1 compatible mode but it receives an MLDv2 Query. vRtrMld HostAddress will identify the Host on which the query is received. vRtr MldHostOperVersion will indicate the compatibility mode of the Host and vRtrMldNotifyQueryVersion will contain the version of the received query.
Effect	N/A
Recovery	N/A

41.8 vRtrMldHostInstantiationFail

Table 743: vRtrMldHostInstantiationFail properties

Property name	Value
Application name	MLD
Event ID	2005
Event name	vRtrMldHostInstantiationFail
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.5
Default severity	warning
Message format string	MLD cannot be started on host because *$vRtrMldNotifyDescription$*
Cause	The vRtrMldHostInstantiationFail event is generated when a host is eligible for running MLD, but MLD cannot be started on the host.
Effect	N/A
Recovery	N/A

41.9 vRtrMldHostMaxGrpsLimitExceeded

Table 744: vRtrMldHostMaxGrpsLimitExceeded properties

Property name	Value
Application name	MLD
Event ID	2006
Event name	vRtrMldHostMaxGrpsLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.6
Default severity	warning
Message format string	*$vRtrMldHostMaxGroups$* exceeded on FwdSvdId *$vRtrMldHostFwd SvcId$*, GrpIfId *$vRtrMldHostGrpIfId$*
Cause	The vRtrMldMaxGrpsLimitExceeded event is generated when an attempt is made to configure a group when vRtrMldHostGroupCount, the number of groups configured on the PIM interface, is equal to vRtr MldHostMaxGroups, the maximum number of groups supported on the host.
Effect	N/A
Recovery	N/A

41.10 vRtrMldHostMaxGrpSrcsLimitExcd

Table 745: vRtrMldHostMaxGrpSrcsLimitExcd properties

Property name	Value
Application name	MLD
Event ID	2017
Event name	vRtrMldHostMaxGrpSrcsLimitExcd
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.17
Default severity	warning
Message format string	Max group sources *$vRtrMldHostMaxGrpSources$* exceeded on Grp IfId *$vRtrMldHostGrpIfId$* with FwdSvcId *$vRtrMldHostFwdSvcId$*
Cause	The vRtrMldHostMaxGrpSrcsLimitExcd event is generated when an attempt is made to configure a source for a group when the number of

Property name	Value
	group sources is equal to vRtrMldHostMaxGrpSources, the maximum number of group sources per group supported on the host.
Effect	N/A
Recovery	N/A

41.11 vRtrMldHostMaxSrcsLimitExceeded

Table 746: vRtrMldHostMaxSrcsLimitExceeded properties

Property name	Value
Application name	MLD
Event ID	2010
Event name	vRtrMldHostMaxSrcsLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.10
Default severity	warning
Message format string	Max group sources limit of *$vRtrMldHostMaxSources$* exceeded on GrpIfId *$vRtrMldHostGrpIfId$* with FwdSvcId *$vRtrMldHostFwdSvcId$*
Cause	The vRtrMldHostMaxSrcsLimitExceeded event is generated when an attempt is made to configure a source for a group when the number of sources for this group is equal to vRtrMldHostMaxSources, the maximum number of sources per group supported on the host.
Effect	N/A
Recovery	N/A

41.12 vRtrMldHostMcacPlcyDropped

Table 747: vRtrMldHostMcacPlcyDropped properties

Property name	Value
Application name	MLD
Event ID	2007
Event name	vRtrMldHostMcacPlcyDropped

Property name	Value
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.7
Default severity	warning
Message format string	MLD group *$vRtrMldNotifyGrpAddr$* dropped on host *$vRtrMldHost SubscriberId$* after applying plcy *$vRtrMldNotifyMcacPolicyName$*
Cause	The vRtrMldHostMcacPlcyDropped event is generated when an MLD group is dropped on a given Host because of applying a multicast CAC policy given by vRtrMldNotifyMcacPolicyName.
Effect	N/A
Recovery	N/A

41.13 vRtrMldHostQryIntervalConflict

Table 748: vRtrMldHostQryIntervalConflict properties

Property name	Value
Application name	MLD
Event ID	2020
Event name	vRtrMldHostQryIntervalConflict
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.20
Default severity	warning
Message format string	TODO
Cause	The vRtrMldHostQryIntervalConflict event is generated when one of the MLD-policy query intervals violates restrictions, we fall back to the node query intervals.
Effect	N/A
Recovery	N/A

41.14 vRtrMldHostRxQueryVerMismatch

Table 749: vRtrMldHostRxQueryVerMismatch properties

Property name	Value
Application name	MLD
Event ID	2009
Event name	vRtrMldHostRxQueryVerMismatch
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.9
Default severity	warning
Message format string	Host MLD version *$vRtrMldHostAdminVersion$* received query version *$vRtrMldNotifyQueryVersion$*
Cause	A vRtrMldHostRxQueryVerMismatch notification is generated when the MLD host is configured as MLDv2 but receives a MLDv1 Query. vRtr MldHostAddress will identify the Host on which the query is received. v RtrMldHostAdminVersion will contain the configured version of the Host and vRtrMldNotifyQueryVersion will contain the version of the received query.
Effect	N/A
Recovery	N/A

41.15 vRtrMldIfCModeRxQueryMismatch

Table 750: vRtrMldIfCModeRxQueryMismatch properties

Property name	Value
Application name	MLD
Event ID	2002
Event name	vRtrMldIfCModeRxQueryMismatch
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.2
Default severity	warning
Message format string	Mismatch between the interface *$vRtrIfIndex$* compatible mode(*$vRtr MldIfOperVersion$*) and the version of the MLD query (version *$vRtr MldNotifyQueryVersion$*) received on the interface

Property name	Value
Cause	This notification is generated when there is a mismatch between the compatibility mode of the interface and the version of the MLD query received on the interface.
Effect	The query will be ignored
Recovery	No recovery is necessary.

41.16 vRtrMldIfRxQueryVerMismatch

Table 751: vRtrMldIfRxQueryVerMismatch properties

Property name	Value
Application name	MLD
Event ID	2001
Event name	vRtrMldIfRxQueryVerMismatch
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.1
Default severity	warning
Message format string	MLDv*$vRtrMldNotifyQueryVersion$* query received on interface *$vRtrIfIndex$* configured as MLDv*$vRtrMldIfAdminVersion$*
Cause	The event is generated when the router receives MLDv1 query on an interface which is configured as MLDv2.
Effect	MLD interface transitions into MLDv1 or MLDv2 compatibility mode.
Recovery	No recovery is necessary.

41.17 vRtrMldMaxGrpsLimitExceeded

Table 752: vRtrMldMaxGrpsLimitExceeded properties

Property name	Value
Application name	MLD
Event ID	2003
Event name	vRtrMldMaxGrpsLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.3

Property name	Value
Default severity	warning
Message format string	The number of groups configured on the interface *$ifName$* has exceeded the maximum limit of *$vRtrMldIfMaxGroups$*
Cause	This notification is generated when the number of groups configured on the interface exceeds the maximum number of groups supported on the system.
Effect	N/A
Recovery	N/A

41.18 vRtrMldMaxGrpSrcsLimitExceeded

Table 753: vRtrMldMaxGrpSrcsLimitExceeded properties

Property name	Value
Application name	MLD
Event ID	2018
Event name	vRtrMldMaxGrpSrcsLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.18
Default severity	warning
Message format string	Max group sources exceeded *$vRtrMldIfMaxGrpSources$* for interface
Cause	The vRtrMldMaxGrpSrcsLimitExceeded event is generated when an attempt is made to configure a group source for a group when the number of group sources is equal to vRtrMldIfMaxGrpSources, the maximum number of group sources per group supported on the interface.
Effect	N/A
Recovery	N/A

41.19 vRtrMldMaxSrcsLimitExceeded

Table 754: vRtrMldMaxSrcsLimitExceeded properties

Property name	Value
Application name	MLD
Event ID	2011
Event name	vRtrMldMaxSrcsLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.11
Default severity	warning
Message format string	Max group sources *$vRtrMldIfMaxSources$* exceeded on interface
Cause	The vRtrMldMaxSrcsLimitExceeded event is generated when an attempt is made to configure a source for a group when the number of sources for this group is equal to vRtrMldIfMaxSources, the maximum number of sources per group supported on the interface.
Effect	N/A
Recovery	N/A

41.20 vRtrMldMcacPlcyDropped

Table 755: vRtrMldMcacPlcyDropped properties

Property name	Value
Application name	MLD
Event ID	2004
Event name	vRtrMldMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.4
Default severity	warning
Message format string	MLD group *$vRtrMldNotifyGrpAddr$* dropped after applying *$vRtrMldIfMcacPolicyName$*
Cause	The vRtrMldMcacPlcyDropped event is generated when an MLD group is dropped on a given interface because of applying a multicast CAC policy given by vRtrMldIfMcacPolicyName.
Effect	N/A

Property name	Value
Recovery	N/A

42 MLD_SNOOPING

42.1 sapMldSnpgGrpLimitExceeded

Table 756: sapMldSnpgGrpLimitExceeded properties

Property name	Value
Application name	MLD_SNOOPING
Event ID	2001
Event name	sapMldSnpgGrpLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-SNOOPING-MIB.tmnxMldSnpgSapNotifications.1
Default severity	warning
Message format string	The number of groups on SAP *$sapEncapValue$* in service *$svcId$* has exceeded the maximum limit of *$sapMldSnpgCfgMaxNbrGrps$* - Dropping group *$tmnxMldSnpgGroupAddress$*
Cause	A MLD group is dropped on a given SAP because a user configurable upper limit given by sapMldSnpgCfgMaxNbrGrps has been reached.
Effect	N/A
Recovery	N/A

42.2 sapMldSnpgMcsFailure

Table 757: sapMldSnpgMcsFailure properties

Property name	Value
Application name	MLD_SNOOPING
Event ID	2003
Event name	sapMldSnpgMcsFailure
SNMP notification prefix and OID	TIMETRA-MLD-SNOOPING-MIB.tmnxMldSnpgSapNotifications.2
Default severity	warning

Property name	Value
Message format string	Group *$tmnxMldSnpgGroupAddress$* on SAP *$sapEncapValue$* in service *$svcId$* could not be synced to MCS - *$tmnxMldSnpgMcsFailureReason$*
Cause	A MLD group on a given SAP could not be synced to the MCS (multi-chassis synchronization) database.
Effect	N/A
Recovery	N/A

42.3 sdpBndMldSnpgGrpLimitExceeded

Table 758: sdpBndMldSnpgGrpLimitExceeded properties

Property name	Value
Application name	MLD_SNOOPING
Event ID	2002
Event name	sdpBndMldSnpgGrpLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-SNOOPING-MIB.tmnxMldSnpgSdpBndNotifications.1
Default severity	warning
Message format string	The number of groups on SDP Bind *$sdpBindId$* in service *$svcId$* has exceeded the maximum limit of *$sdpBndMldSnpgCfgMaxNbrGrps$* - Dropping group *$tmnxMldSnpgGroupAddress$*
Cause	A MLD group is dropped on a given SDP bind because a user configurable upper limit given by sdpBndMldSnpgCfgMaxNbrGrps is reached.
Effect	N/A
Recovery	N/A

43 MPLS

43.1 mplsTunnelDown

Table 759: mplsTunnelDown properties

Property name	Value
Application name	MPLS
Event ID	2004
Event name	mplsTunnelDown
SNMP notification prefix and OID	MPLS-TE-MIB.mplsTeNotifyPrefix.2
Default severity	warning
Message format string	Tunnel *$mplsTunnelName$* is operationally disabled ('shutdown')
Cause	An mplsTunnelOperStatus object for one of the configured tunnels is about to enter the down state from some other state (besides the not Present state). This other state is indicated by the included value of mplsTunnelOperStatus.
Effect	Service is affected.
Recovery	No recovery is required.

43.2 mplsTunnelReoptimized

Table 760: mplsTunnelReoptimized properties

Property name	Value
Application name	MPLS
Event ID	2006
Event name	mplsTunnelReoptimized
SNMP notification prefix and OID	MPLS-TE-MIB.mplsTeNotifyPrefix.4
Default severity	warning
Message format string	Tunnel *$mplsTunnelName$* is reoptimized

Property name	Value
Cause	A tunnel is reoptimized. If the actual path is used, then this object MAY contain the new path for this tunnel some time after this trap is issued by the agent.
Effect	Service is affected.
Recovery	No recovery is required.

43.3 mplsTunnelRerouted

Table 761: mplsTunnelRerouted properties

Property name	Value
Application name	MPLS
Event ID	2005
Event name	mplsTunnelRerouted
SNMP notification prefix and OID	MPLS-TE-MIB.mplsTeNotifyPrefix.3
Default severity	warning
Message format string	Tunnel *$mplsTunnelName$* is rerouted
Cause	A tunnel is rerouted or re-optimized. If the Actual Path is used, then this object MAY contain the new path for this tunnel some time after this trap is issued by the agent.
Effect	Service is affected.
Recovery	No recovery is required.

43.4 mplsTunnelUp

Table 762: mplsTunnelUp properties

Property name	Value
Application name	MPLS
Event ID	2003
Event name	mplsTunnelUp
SNMP notification prefix and OID	MPLS-TE-MIB.mplsTeNotifyPrefix.1

Property name	Value
Default severity	warning
Message format string	Tunnel *$mplsTunnelName$* is operationally enabled ('no shutdown')
Cause	An mplsTunnelOperStatus object for one of the configured tunnels is about to leave the down state and transition into some other state (but not into the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus.
Effect	Service is affected.
Recovery	No recovery is required.

43.5 mplsXCDown

Table 763: mplsXCDown properties

Property name	Value
Application name	MPLS
Event ID	2002
Event name	mplsXCDown
SNMP notification prefix and OID	MPLS-LSR-MIB.mplsLsrNotifyPrefix.2
Default severity	warning
Message format string	Cross-connect *$mplsXCName$* is down
Cause	An mplsXCOperStatus object for one of the configured cross-connect entries is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of mplsXCOperStatus.
Effect	Service is affected.
Recovery	No recovery is required.

43.6 mplsXCUp

Table 764: mplsXCUp properties

Property name	Value
Application name	MPLS

Property name	Value
Event ID	2001
Event name	mplsXCUp
SNMP notification prefix and OID	MPLS-LSR-MIB.mplsLsrNotifyPrefix.1
Default severity	warning
Message format string	Cross-connect *$mplsXCName$* is up
Cause	An mplsXCOperStatus object for one of the configured cross-connect entries is about to leave the down state and transition into some other state (but not into the notPresent state). This other state is indicated by the included value of mplsXCOperStatus.
Effect	Service is affected.
Recovery	No recovery is required.

43.7 vRtrMplsIfStateChange

Table 765: vRtrMplsIfStateChange properties

Property name	Value
Application name	MPLS
Event ID	2008
Event name	vRtrMplsIfStateChange
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.2
Default severity	warning
Message format string	Interface *$vRtrIfIndex$* is in administrative state: *$vRtrMplsIfAdmin State$*, operational state: *$vRtrMplsIfOperState$*
Cause	The MPLS interface changed state.
Effect	Service is affected.
Recovery	No recovery is required.

43.8 vRtrMplsLspActivePathChanged

Table 766: vRtrMplsLspActivePathChanged properties

Property name	Value
Application name	MPLS
Event ID	2027
Event name	vRtrMplsLspActivePathChanged
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.21
Default severity	minor
Message format string	Possible messages: • LSP *$lspName$* active path *$lspOldPathName$* has changed to active path *$lspPathName$* • LSP *$lspName$* active path *$lspOldPathName$* has changed to active path *$lspPathName$* by manual method *$vRtrMplsLspPath ActiveByManual$*
Cause	The vRtrMplsLspActivePathChanged notification is generated when the active path of an LSP successfully switches to an new path. This notification will also be sent when the active LSP path does not change but only the switch method changes on the path. The old LSP path index is specified by vRtrMplsLspOldTunnelIndex. The state and switch method of the current active LSP path are specified by vRtrMplsLsp PathState and vRtrMplsLspPathActiveByManual respectively.
Effect	The switchover to the new LSP path was successful and/or the switch method of the current active LSP path changed.
Recovery	There is no recovery required for this notification.

43.9 vRtrMplsLspDown

Table 767: vRtrMplsLspDown properties

Property name	Value
Application name	MPLS
Event ID	2010
Event name	vRtrMplsLspDown
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.4

Property name	Value
Default severity	warning
Message format string	LSP *$lspName$* is operationally disabled ('shutdown') because *$vRtr MplsLspNotificationReasonCode$*
Cause	An LSP transitioned out of 'inService' state to any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.10 vRtrMplsLspPathDown

Table 768: vRtrMplsLspPathDown properties

Property name	Value
Application name	MPLS
Event ID	2012
Event name	vRtrMplsLspPathDown
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.6
Default severity	warning
Message format string	LSP path *$lspPathName$* is operationally disabled ('shutdown') because *$vRtrMplsLspPathNotificationReasonCode$*
Cause	A LSP Path transitioned out of 'inService' state to any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.11 vRtrMplsLspPathLstFillReoptElig

Table 769: vRtrMplsLspPathLstFillReoptElig properties

Property name	Value
Application name	MPLS
Event ID	2022
Event name	vRtrMplsLspPathLstFillReoptElig

Property name	Value
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.16
Default severity	warning
Message format string	Better least-fill metric for path *$lspPathName$* is *$trapStatus$*. *$bandwidthChange$*
Cause	The vRtrMplsLspPathLstFillReoptElig notification is set/reset based on when a timer based re-signal found/did not find a path with the same cost but which has a better least-fill metric.
Effect	N/A
Recovery	N/A

43.12 vRtrMplsLspPathMbbStatusEvent

Table 770: vRtrMplsLspPathMbbStatusEvent properties

Property name	Value
Application name	MPLS
Event ID	2025
Event name	vRtrMplsLspPathMbbStatusEvent
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.19
Default severity	warning
Message format string	*$vRtrMplsLspPathLastMBBType$* MBB *$vRtrMplsLspPathMbbStatus$* for LSP path *$lspPathName$* - reason *$vRtrMplsLspPathMbbReason Code$*
Cause	Status of the make-before-break(MBB) operation for the LSP path has changed.
Effect	N/A
Recovery	N/A

43.13 vRtrMplsLspPathRerouted

Table 771: vRtrMplsLspPathRerouted properties

Property name	Value
Application name	MPLS
Event ID	2013
Event name	vRtrMplsLspPathRerouted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.7
Default severity	warning
Message format string	LSP path *$lspPathName$* rerouted
Cause	An LSP Path has been rerouted.
Effect	N/A
Recovery	N/A

43.14 vRtrMplsLspPathResignaled

Table 772: vRtrMplsLspPathResignaled properties

Property name	Value
Application name	MPLS
Event ID	2014
Event name	vRtrMplsLspPathResignaled
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.8
Default severity	warning
Message format string	LSP path *$lspPathName$* resignaled as a result of *$vRtrMplsLspPath LastMBBType$* MBB
Cause	An LSP Path has resignaled.
Effect	N/A
Recovery	N/A

43.15 vRtrMplsLspPathSoftPreempted

Table 773: vRtrMplsLspPathSoftPreempted properties

Property name	Value
Application name	MPLS
Event ID	2021
Event name	vRtrMplsLspPathSoftPreempted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.15
Default severity	warning
Message format string	LSP path *$lspPathName$* preempted
Cause	The vRtrMplsLspPathSoftPreempted notification is generated when an LSP Path is preempted.
Effect	N/A
Recovery	N/A

43.16 vRtrMplsLspPathUp

Table 774: vRtrMplsLspPathUp properties

Property name	Value
Application name	MPLS
Event ID	2011
Event name	vRtrMplsLspPathUp
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.5
Default severity	warning
Message format string	LSP path *$lspPathName$* is operationally enabled ('no shutdown')
Cause	A LSP Path transitioned to the 'inService' state from any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.17 vRtrMplsLspSwitchStbyFailure

Table 775: vRtrMplsLspSwitchStbyFailure properties

Property name	Value
Application name	MPLS
Event ID	2026
Event name	vRtrMplsLspSwitchStbyFailure
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.20
Default severity	warning
Message format string	Switchover to standby path with tunnel index *$vRtrMplsLspSwitchStbyPathIndex$* for lsp *$lspName$* failed because *$vRtrMplsLspSwitchStbyReasonCode$*
Cause	The vRtrMplsLspSwitchStbyFailure notification is generated to report an unsuccessful switchover from the current active secondary LSP path of an LSP to another secondary standby LSP path. The reason for the failure is specified by vRtrMplsLspSwitchStbyReasonCode.
Effect	The switchover to the new standby path failed for the LSP.
Recovery	The vRtrMplsLspSwitchStbyReasonCode will help the user troubleshoot the failure. The user can attempt to switchover to another standby LSP path again.

43.18 vRtrMplsLspUp

Table 776: vRtrMplsLspUp properties

Property name	Value
Application name	MPLS
Event ID	2009
Event name	vRtrMplsLspUp
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.3
Default severity	warning
Message format string	LSP *$lspName$* is operationally enabled ('no shutdown')
Cause	A LSP transitioned to the 'inService' state from any other state.
Effect	Service is affected.

Property name	Value
Recovery	No recovery is required.

43.19 vRtrMplsNodeInIgpOverload

Table 777: vRtrMplsNodeInIgpOverload properties

Property name	Value
Application name	MPLS
Event ID	2030
Event name	vRtrMplsNodeInIgpOverload
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.24
Default severity	minor
Message format string	MPLS received a notification that *$vRtrMplsIgpOverloadIgpType$* is in overload on router *$vRtrMplsIgpOverloadRtrAddr$*.
Cause	The vRtrMplsNodeInIgpOverload notification is generated when MPLS gets a notification that a node is in IGP overload state.
Effect	The LSPs transiting through nodes that are in IGP overload state are teardown.
Recovery	There is no recovery required for this notification.

43.20 vRtrMplsP2mpInstanceDown

Table 778: vRtrMplsP2mpInstanceDown properties

Property name	Value
Application name	MPLS
Event ID	2016
Event name	vRtrMplsP2mpInstanceDown
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.10
Default severity	warning
Message format string	P2MP instance *$insName$* LSP *$lspName$* is operationally disabled ('shutdown') because *$vRtrMplsP2mpInstNotifReasonCode$*

Property name	Value
Cause	A P2MP instance under LSP transitioned out of 'inService' state to any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.21 vRtrMplsP2mpInstanceResignaled

Table 779: vRtrMplsP2mpInstanceResignaled properties

Property name	Value
Application name	MPLS
Event ID	2023
Event name	vRtrMplsP2mpInstanceResignaled
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.17
Default severity	warning
Message format string	P2MP instance *$insName$* LSP *$lspName$* has been resignaled as a result of *$vRtrMplsP2mpInstLastMBBType$* MBB
Cause	A P2MP instance was resignaled.
Effect	Service is affected.
Recovery	No recovery is required.

43.22 vRtrMplsP2mpInstanceUp

Table 780: vRtrMplsP2mpInstanceUp properties

Property name	Value
Application name	MPLS
Event ID	2015
Event name	vRtrMplsP2mpInstanceUp
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.9
Default severity	warning

Property name	Value
Message format string	P2MP instance *$insName$* LSP *$lspName$* is operationally enabled ('no shutdown')
Cause	A P2MP instance under LSP transitioned to the 'inService' state from any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.23 vRtrMplsResignalTimerExpired

Table 781: vRtrMplsResignalTimerExpired properties

Property name	Value
Application name	MPLS
Event ID	2024
Event name	vRtrMplsResignalTimerExpired
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.18
Default severity	warning
Message format string	MPLS resignal timer expired.
Cause	MPLS resignal timer expired
Effect	N/A
Recovery	No recovery is required.

43.24 vRtrMplsS2lSubLspDown

Table 782: vRtrMplsS2lSubLspDown properties

Property name	Value
Application name	MPLS
Event ID	2018
Event name	vRtrMplsS2lSubLspDown
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.12

Property name	Value
Default severity	warning
Message format string	S2L path *$s2lName$* to *$vRtrMplsS2lSubLspNtDstAddr$* for P2MP instance *$insName$* LSP *$lspName$* is operationally disabled ('shutdown') because *$vRtrMplsS2lSubLspFailCode$*
Cause	A S2L Path transitioned out of 'inService' state to any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.25 vRtrMplsS2lSubLspRerouted

Table 783: vRtrMplsS2lSubLspRerouted properties

Property name	Value
Application name	MPLS
Event ID	2019
Event name	vRtrMplsS2lSubLspRerouted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.13
Default severity	warning
Message format string	S2L path *$s2lName$* to *$vRtrMplsS2lSubLspNtDstAddr$* for P2MP instance *$insName$* for LSP *$lspName$* rerouted
Cause	An S2L Path was rerouted.
Effect	N/A
Recovery	N/A

43.26 vRtrMplsS2lSubLspResignaled

Table 784: vRtrMplsS2lSubLspResignaled properties

Property name	Value
Application name	MPLS
Event ID	2020

Property name	Value
Event name	vRtrMplsS2lSubLspResignaled
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.14
Default severity	warning
Message format string	S2L path *$s2lName$* to *$vRtrMplsS2lSubLspNtDstAddr$* for P2MP instance *$insName$* LSP *$lspName$* resignaled as a result of *$vRtr MplsS2lSubLspLastMBBType$* MBB
Cause	An S2L Path was resignaled.
Effect	N/A
Recovery	N/A

43.27 vRtrMplsS2lSubLspUp

Table 785: vRtrMplsS2lSubLspUp properties

Property name	Value
Application name	MPLS
Event ID	2017
Event name	vRtrMplsS2lSubLspUp
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.11
Default severity	warning
Message format string	S2L path *$s2lName$* to *$vRtrMplsS2lSubLspNtDstAddr$* for P2MP instance *$insName$* LSP *$lspName$* is operationally enabled ('no shutdown')
Cause	A S2L Path transitioned to the 'inService' state from any other state.
Effect	Service is affected.
Recovery	No recovery is required.

43.28 vRtrMplsStateChange

Table 786: vRtrMplsStateChange properties

Property name	Value
Application name	MPLS
Event ID	2007
Event name	vRtrMplsStateChange
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.1
Default severity	warning
Message format string	Instance is in administrative state: *$vRtrMplsGeneralAdminState$*, operational state: *$vRtrMplsGeneralOperState$*
Cause	The MPLS module changed state.
Effect	Service is affected.
Recovery	No recovery is required.

43.29 vRtrMplsXCBundleChange

Table 787: vRtrMplsXCBundleChange properties

Property name	Value
Application name	MPLS
Event ID	2028
Event name	vRtrMplsXCBundleChange
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.22
Default severity	minor
Message format string	*$vRtrMplsXCNotifyRednNumOfBitsSet$* RSVP sessions *$vRtr MplsXCNotifyRednBundlingType$* starting from session number *$vRtr MplsXCNotifyRednStartIndex$* to *$vRtrMplsXCNotifyRednEndIndex$*
Cause	vRtrMplsXCBundleChange is generated when one or more RSVP sessions changed state and retained the changed state for an entire quiet interval of 2 minutes or the maximum interval of 10 minutes if the state of RSVP sessions kept on changing during this period of multiple quiet intervals.

Property name	Value
Effect	RSVP sessions represented by bits in vRtrMplsXCNotifRednIndicesBit Map changed state on this router instance.
Recovery	There is no recovery required for this notification.

44 MPLS_TP

44.1 vRtrMplsTpLspActivePathChange

Table 788: vRtrMplsTpLspActivePathChange properties

Property name	Value
Application name	MPLS_TP
Event ID	2006
Event name	vRtrMplsTpLspActivePathChange
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.6
Default severity	minor
Message format string	TP Tunnel *$TpLspName$* switched from *$vRtrMplsTpLspOldPathIndex $* to *$vRtrMplsTpLspPathIndex$* path
Cause	The vRtrMplsTpLspActivePathChange notification is generated when a MPLS-TP LSP Path changes its path from working to protecting or visa versa. The old path is specified by vRtrMplsTpLspOldPathIndex.
Effect	The TP Path after the switch will be used to transport user traffic.
Recovery	There is no recovery required for this notification.

44.2 vRtrMplsTpLspActivePathUp

Table 789: vRtrMplsTpLspActivePathUp properties

Property name	Value
Application name	MPLS_TP
Event ID	2005
Event name	vRtrMplsTpLspActivePathUp
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.5
Default severity	minor
Message format string	TP Tunnel *$TpLspName$* active on *$vRtrMplsTpLspPathIndex$* path

Property name	Value
Cause	The vRtrMplsTpLspActivePathUp notification is generated when a MPLS-TP LSP Path comes up.
Effect	The TP-Path is the active path in the tunnel that is used to transport user traffic.
Recovery	There is no recovery required for this notification.

44.3 vRtrMplsTpLspPtTypeMismatchAlarm

Table 790: vRtrMplsTpLspPtTypeMismatchAlarm properties

Property name	Value
Application name	MPLS_TP
Event ID	2003
Event name	vRtrMplsTpLspPtTypeMismatchAlarm
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.3
Default severity	minor
Message format string	MPLS-TP Tunnel *$vRtrMplsLspIndex$* experiencing protection type mismatch: Rx 0x*$vRtrMplsTpLspPtPathMepRxPdu$* Tx 0x *$vRtrMplsTpLspPtPathMepTxPdu$*
Cause	The vRtrMplsTpLspPtTypeMismatchAlarm is generated when an MPLS-TP LSP protection type mismatch is detected on the protection MEP, at the APS layer, by comparing the PT bits of the transmitted and received APS protocol.
Effect	N/A
Recovery	N/A

44.4 vRtrMplsTpLspPtTypeMismatchClear

Table 791: vRtrMplsTpLspPtTypeMismatchClear properties

Property name	Value
Application name	MPLS_TP
Event ID	2004

Property name	Value
Event name	vRtrMplsTpLspPtTypeMismatchClear
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.4
Default severity	minor
Message format string	MPLS-TP Tunnel *$vRtrMplsLspIndex$* experiencing protection type mismatch cleared: Rx 0x *$vRtrMplsTpLspPtPathMepRxPdu$* Tx 0x*$vRtrMplsTpLspPtPathMepTxPdu$*
Cause	The vRtrMplsTpLspPtTypeMismatchClear is generated when an MPLS-TP LSP protection type mismatch is cleared.
Effect	N/A
Recovery	N/A

44.5 vRtrMplsTpLspRevertMismatchAlarm

Table 792: vRtrMplsTpLspRevertMismatchAlarm properties

Property name	Value
Application name	MPLS_TP
Event ID	2001
Event name	vRtrMplsTpLspRevertMismatchAlarm
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.1
Default severity	minor
Message format string	MPLS-TP Tunnel *$vRtrMplsLspIndex$* experiencing revertive mode mismatch: Rx 0x*$vRtrMplsTpLspPtPathMepRxPdu$* Tx 0x *$vRtrMplsTpLspPtPathMepTxPdu$*
Cause	The vRtrMplsTpLspRevertMismatchAlarm is generated when an MPLS-TP LSP revertive mode mismatch is detected on the protection MEP, at the APS layer, by comparing the R bit of the transmitted and received APS protocol.
Effect	N/A
Recovery	N/A

44.6 vRtrMplsTpLspRevertMismatchClear

Table 793: vRtrMplsTpLspRevertMismatchClear properties

Property name	Value
Application name	MPLS_TP
Event ID	2002
Event name	vRtrMplsTpLspRevertMismatchClear
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.2
Default severity	minor
Message format string	MPLS-TP Tunnel *$vRtrMplsLspIndex$* experiencing revertive mode mismatch cleared: Rx 0x *$vRtrMplsTpLspPtPathMepRxPdu$* Tx 0x*$vRtrMplsTpLspPtPathMepTxPdu$*
Cause	The vRtrMplsTpLspRevertMismatchClear is generated when an MPLS-TP LSP revertive mode mismatch is cleared.
Effect	N/A
Recovery	N/A

45 MSDP

45.1 msdpBackwardTransition

Table 794: msdpBackwardTransition properties

Property name	Value
Application name	MSDP
Event ID	2002
Event name	msdpBackwardTransition
SNMP notification prefix and OID	MSDP-MIB.msdpTraps.2
Default severity	minor
Message format string	MSDP FSM for peer *$strPeer$* has moved from a higher numbered state to a lower numbered state.
Cause	The MSDP FSM moves from a higher numbered state to a lower numbered state.
Effect	N/A
Recovery	N/A

45.2 msdpEstablished

Table 795: msdpEstablished properties

Property name	Value
Application name	MSDP
Event ID	2001
Event name	msdpEstablished
SNMP notification prefix and OID	MSDP-MIB.msdpTraps.1
Default severity	minor
Message format string	MSDP FSM for peer *$strPeer$* has entered ESTABLISHED state.

Property name	Value
Cause	The MSDP FSM entered the ESTABLISHED state.
Effect	N/A
Recovery	N/A

45.3 tmnxMsdpNgActSrcLimExcd

Table 796: tmnxMsdpNgActSrcLimExcd properties

Property name	Value
Application name	MSDP
Event ID	2008
Event name	tmnxMsdpNgActSrcLimExcd
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.1
Default severity	minor
Message format string	Global active source limit *$tmnxMsdpNgMaxActiveSources$* has been exceeded.Num exceeded *$tmnxMsdpNgStatusActSrcLimExceeded$*.
Cause	The tmnxMsdpNgActSrcLimExcd event is generated whenever the global active source limit has been exceeded.
Effect	N/A
Recovery	N/A

45.4 tmnxMsdpNgGroupSrcActMsgsExcd

Table 797: tmnxMsdpNgGroupSrcActMsgsExcd properties

Property name	Value
Application name	MSDP
Event ID	2012
Event name	tmnxMsdpNgGroupSrcActMsgsExcd
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.5
Default severity	minor

Property name	Value
Message format string	Active source limit *$tmnxMsdpNgPeerGroupMaxActSources$* reached for group *$strGrpPref$*. Num exceeded *$tmnxMsdpNgPeerGroupActMsgsExMax$*
Cause	The tmnxMsdpNgGroupSrcActMsgsExcd event is generated when the source active messages received from this group has exceeded the established maximum number.
Effect	N/A
Recovery	N/A

45.5 tmnxMsdpNgPeerActSrcLimExcd

Table 798: tmnxMsdpNgPeerActSrcLimExcd properties

Property name	Value
Application name	MSDP
Event ID	2009
Event name	tmnxMsdpNgPeerActSrcLimExcd
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.2
Default severity	minor
Message format string	Active source limit *$strLimit$* for peer *$strPeer$* has been exceeded.Num exceeded *$tmnxMsdpNgPeerStatsActSrcLimExcd$*.
Cause	The tmnxMsdpNgPeerActSrcLimExcd event is generated whenever the active source limit has been exceeded for the peer.
Effect	N/A
Recovery	N/A

45.6 tmnxMsdpNgRPFFailure

Table 799: tmnxMsdpNgRPFFailure properties

Property name	Value
Application name	MSDP
Event ID	2010

Property name	Value
Event name	tmnxMsdpNgRPFFailure
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.3
Default severity	minor
Message format string	RPF failure for SA (*$strGrp$*, *$strSrc$*) RP *$strRp$* received from peer *$strPeer$*
Cause	The tmnxMsdpNgRPFFailure event is generated whenever a RPF(Reverse Path Forwarding) failure occurs for a source configured by user.
Effect	N/A
Recovery	N/A

45.7 tmnxMsdpNgSourceSrcActMsgsExcd

Table 800: tmnxMsdpNgSourceSrcActMsgsExcd properties

Property name	Value
Application name	MSDP
Event ID	2011
Event name	tmnxMsdpNgSourceSrcActMsgsExcd
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.4
Default severity	minor
Message format string	Active source limit *$tmnxMsdpNgSourceMaxActiveSources$* reached for source *$strSrcPref$*. Num exceeded *$tmnxMsdpNgSourceSrcAct MsgsExMax$*
Cause	The tmnxMsdpNgSourceSrcActMsgsExcd event is generated when the source active messages received from this source has exceeded the established maximum number.
Effect	N/A
Recovery	N/A

46 MWMGR

46.1 aluMwLinkEPSActivityChange

Table 801: aluMwLinkEPSActivityChange properties

Property name	Value
Application name	MWMGR
Event ID	2018
Event name	aluMwLinkEPSActivityChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.18
Default severity	major
Message format string	Microwave Link EPS Switch
Cause	N/A
Effect	N/A
Recovery	N/A

46.2 aluMwLinkMaintenanceChange

Table 802: aluMwLinkMaintenanceChange properties

Property name	Value
Application name	MWMGR
Event ID	2021
Event name	aluMwLinkMaintenanceChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.21
Default severity	minor
Message format string	Microwave Link maintenance command applied
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.3 aluMwLinkPeerChange

Table 803: aluMwLinkPeerChange properties

Property name	Value
Application name	MWMGR
Event ID	2022
Event name	aluMwLinkPeerChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.22
Default severity	minor
Message format string	Microwave link peer discovered
Cause	N/A
Effect	N/A
Recovery	N/A

46.4 aluMwLinkRPSActivityChange

Table 804: aluMwLinkRPSActivityChange properties

Property name	Value
Application name	MWMGR
Event ID	2020
Event name	aluMwLinkRPSActivityChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.20
Default severity	major
Message format string	Microwave Link RPS Switch
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.5 aluMwLinkTPSActivityChange

Table 805: aluMwLinkTPSActivityChange properties

Property name	Value
Application name	MWMGR
Event ID	2019
Event name	aluMwLinkTPSActivityChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.19
Default severity	major
Message format string	Microwave Link TPS Switch
Cause	N/A
Effect	N/A
Recovery	N/A

46.6 aluMwRadioCriticalAlarmClear

Table 806: aluMwRadioCriticalAlarmClear properties

Property name	Value
Application name	MWMGR
Event ID	2008
Event name	aluMwRadioCriticalAlarmClear
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.8
Default severity	critical
Message format string	Microwave Radio critical alarm cleared
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.7 aluMwRadioCriticalAlarmRaise

Table 807: aluMwRadioCriticalAlarmRaise properties

Property name	Value
Application name	MWMGR
Event ID	2007
Event name	aluMwRadioCriticalAlarmRaise
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.7
Default severity	critical
Message format string	Microwave Radio critcal alarm failure
Cause	N/A
Effect	N/A
Recovery	N/A

46.8 aluMwRadioDatabaseUpdated

Table 808: aluMwRadioDatabaseUpdated properties

Property name	Value
Application name	MWMGR
Event ID	2006
Event name	aluMwRadioDatabaseUpdated
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.6
Default severity	minor
Message format string	Microwave Radio on port *$subject$* database updated
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.9 aluMwRadioIndetermAlarmClear

Table 809: aluMwRadioIndetermAlarmClear properties

Property name	Value
Application name	MWMGR
Event ID	2016
Event name	aluMwRadioIndetermAlarmClear
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.16
Default severity	indeterminate
Message format string	Microwave Radio indeterminate alarm cleared
Cause	N/A
Effect	N/A
Recovery	N/A

46.10 aluMwRadioIndetermAlarmRaise

Table 810: aluMwRadioIndetermAlarmRaise properties

Property name	Value
Application name	MWMGR
Event ID	2015
Event name	aluMwRadioIndetermAlarmRaise
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.15
Default severity	indeterminate
Message format string	Microwave Radio indeterminate alarm raised
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.11 aluMwRadioLinkDown

Table 811: aluMwRadioLinkDown properties

Property name	Value
Application name	MWMGR
Event ID	2002
Event name	aluMwRadioLinkDown
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.2
Default severity	major
Message format string	Microwave Radio Link on port *$subject$* is down
Cause	N/A
Effect	N/A
Recovery	N/A

46.12 aluMwRadioLinkUp

Table 812: aluMwRadioLinkUp properties

Property name	Value
Application name	MWMGR
Event ID	2001
Event name	aluMwRadioLinkUp
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.1
Default severity	major
Message format string	Microwave Radio Link on port *$subject$* is up
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.13 aluMwRadioMajorAlarmClear

Table 813: aluMwRadioMajorAlarmClear properties

Property name	Value
Application name	MWMGR
Event ID	2010
Event name	aluMwRadioMajorAlarmClear
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.10
Default severity	major
Message format string	Microwave Radio major alarm cleared
Cause	N/A
Effect	N/A
Recovery	N/A

46.14 aluMwRadioMajorAlarmRaise

Table 814: aluMwRadioMajorAlarmRaise properties

Property name	Value
Application name	MWMGR
Event ID	2009
Event name	aluMwRadioMajorAlarmRaise
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.9
Default severity	major
Message format string	Microwave Radio major alarm raise
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.15 aluMwRadioMinorAlarmClear

Table 815: aluMwRadioMinorAlarmClear properties

Property name	Value
Application name	MWMGR
Event ID	2012
Event name	aluMwRadioMinorAlarmClear
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.12
Default severity	minor
Message format string	Microwave Radio minor alarm cleared
Cause	N/A
Effect	N/A
Recovery	N/A

46.16 aluMwRadioMinorAlarmRaise

Table 816: aluMwRadioMinorAlarmRaise properties

Property name	Value
Application name	MWMGR
Event ID	2011
Event name	aluMwRadioMinorAlarmRaise
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.11
Default severity	minor
Message format string	Microwave Radio minor alarm raise
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.17 aluMwRadioNotPresent

Table 817: aluMwRadioNotPresent properties

Property name	Value
Application name	MWMGR
Event ID	2004
Event name	aluMwRadioNotPresent
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.4
Default severity	major
Message format string	Microwave Radio on port *$subject$* is not present
Cause	N/A
Effect	N/A
Recovery	N/A

46.18 aluMwRadioPresent

Table 818: aluMwRadioPresent properties

Property name	Value
Application name	MWMGR
Event ID	2003
Event name	aluMwRadioPresent
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.3
Default severity	major
Message format string	Microwave Radio on port *$subject$* is present
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.19 aluMwRadioSwPackageMissing

Table 819: aluMwRadioSwPackageMissing properties

Property name	Value
Application name	MWMGR
Event ID	2005
Event name	aluMwRadioSwPackageMissing
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.5
Default severity	major
Message format string	No valid Microwave Software Package found
Cause	N/A
Effect	N/A
Recovery	N/A

46.20 aluMwRadioSwStateChange

Table 820: aluMwRadioSwStateChange properties

Property name	Value
Application name	MWMGR
Event ID	2023
Event name	aluMwRadioSwStateChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.23
Default severity	minor
Message format string	Microwave Radio on port *$subject$* software state changed
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.21 aluMwRadioTxChange

Table 821: aluMwRadioTxChange properties

Property name	Value
Application name	MWMGR
Event ID	2017
Event name	aluMwRadioTxChange
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.17
Default severity	major
Message format string	Microwave Radio transmitter is muted
Cause	N/A
Effect	N/A
Recovery	N/A

46.22 aluMwRadioWarningAlarmClear

Table 822: aluMwRadioWarningAlarmClear properties

Property name	Value
Application name	MWMGR
Event ID	2014
Event name	aluMwRadioWarningAlarmClear
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.14
Default severity	warning
Message format string	Microwave Radio warning alarm cleared
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

46.23 aluMwRadioWarningAlarmRaise

Table 823: aluMwRadioWarningAlarmRaise properties

Property name	Value
Application name	MWMGR
Event ID	2013
Event name	aluMwRadioWarningAlarmRaise
SNMP notification prefix and OID	ALU-MICROWAVE-MIB.aluMwNotification.13
Default severity	warning
Message format string	Microwave Radio warning alarm raise
Cause	N/A
Effect	N/A
Recovery	N/A

47 NAT

47.1 tmnxNatDetMapOperStateChanged

Table 824: tmnxNatDetMapOperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2033
Event name	tmnxNatDetMapOperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.33
Default severity	minor
Message format string	The state of deterministic prefix map *$tmnxNatDetPlcyAddr$*/*$tmnxNatDetPlcyAddrPrefixLength$* type *$tmnxNatDetPlcySubType$* start *$tmnxNatDetMapInStart$* end *$tmnxNatDetMapInEnd$* changed to *$tmnxNatDetMapOperState$* - *$tmnxNatNotifyDescription$*
Cause	The tmnxNatDetMapOperStateChanged notification is sent when the value of the object tmnxNatDetMapOperState changes. The cause is explained in the tmnxNatNotifyDescription.
Effect	N/A
Recovery	N/A

47.2 tmnxNatDetPlcyChanged

Table 825: tmnxNatDetPlcyChanged properties

Property name	Value
Application name	NAT
Event ID	2022
Event name	tmnxNatDetPlcyChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.22
Default severity	minor

Property name	Value
Message format string	The Deterministic NAT map has changed.
Cause	Such a change may be caused by a modification of the tmnxNatDet PlcyTable or the tmnxNatDetMapTable.
Effect	Traffic flows of one or more given subscribers, subject to NAT, may be assigned a different outside IP address and/or outside port.
Recovery	Managers that rely on the offline representation of the Deterministic NAT map should get an updated copy.

47.3 tmnxNatDetPlcyOperStateChanged

Table 826: tmnxNatDetPlcyOperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2032
Event name	tmnxNatDetPlcyOperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.32
Default severity	minor
Message format string	The state of deterministic prefix *$tmnxNatDetPlcyAddr$*/*$tmnxNatDet PlcyAddrPrefixLength$* type *$tmnxNatDetPlcySubType$* changed to *$tmnxNatDetPlcyOperState$ - $tmnxNatNotifyDescription$*
Cause	The tmnxNatDetPlcyOperStateChanged notification is sent when the value of the object tmnxNatDetPlcyOperState changes. The cause is explained in the tmnxNatNotifyDescription.
Effect	N/A
Recovery	N/A

47.4 tmnxNatFwd2EntryAdded

Table 827: tmnxNatFwd2EntryAdded properties

Property name	Value
Application name	NAT

Property name	Value
Event ID	2031
Event name	tmnxNatFwd2EntryAdded
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.31
Default severity	minor
Message format string	{*$tmnxNatNotifyPlSeqNum$*} *$tmnxNatNotifyTruthValue$ $tmnxNat Fwd2OutAddr$* [*$tmnxNatFwd2OutPort$*] -- subscriber type <type> {<inside router> <inside IP> [AFTR *$tmnxNatFwd2LsnAftrAddr$*| <subscriber id> } <inside port> <protocol> from *$tmnxNatFwd2Origin$*
Cause	The tmnxNatFwd2EntryAdded notification is sent when a row is added to or removed from the tmnxNatFwd2Table; a row can be added to the table either by operations on the tmnxNatFwdAction object group or by means of the PCP protocol. When the row is added, the value of the object tmnxNatNotifyTruthValue is 'true'; when the row is removed, it is 'false'.
Effect	The specified NAT subscriber can start receiving inbound traffic flows.
Recovery	No recovery required; this notification is the result of an operator or protocol action.

47.5 tmnxNatFwd2OperStateChanged

Table 828: tmnxNatFwd2OperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2034
Event name	tmnxNatFwd2OperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.34
Default severity	warning
Message format string	The state of forwarding entry subscriber type <type> {<inside router> <inside IP> subscriber *$tmnxNatFwd2L2awSubIdent$* } IP protocol *$tmnxNatFwd2Protocol$* inside port *$tmnxNatFwd2Port$* policy *$tmnx NatFwd2NatPolicy$* changed to *$tmnxNatFwd2OperState$*
Cause	The tmnxNatFwd2OperStateChanged notification is sent when the value of the object tmnxNatFwd2OperState changes. This is related to the state of the ISA MDA where the forwarding entry is located, or the availability of resources on that MDA. In the case of Layer-2-

Property name	Value
	Aware NAT subscribers, the tmnxNatFwd2OperState is 'down' while the subscriber is not instantiated. This would typically be a transient situation.
Effect	The corresponding inward bound packets are dropped while the operational status is 'down'.
Recovery	If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.

47.6 tmnxNatInAddrPrefixBlksFree

Table 829: tmnxNatInAddrPrefixBlksFree properties

Property name	Value
Application name	NAT
Event ID	2030
Event name	tmnxNatInAddrPrefixBlksFree
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.30
Default severity	minor
Message format string	{*$tmnxNatNotifyPlSeqNum$*} all blocks freed of all subscribers type *$tmnxNatNotifySubscriberType$* in inside router instance *$tmnxNatNotifyInsideVRtrID$* address type *$tmnxNatNotifyInsideAddrType$* prefix *$tmnxNatNotifyInsideAddr$*/ *$tmnxNatNotifyInsideAddrPrefixLen$* MDA *$tmnxNatNotifyMdaCardSlotNum$*/ *$tmnxNatNotifyMdaSlotNum$* at *$tmnxNatNotifyDateAndTime$* - *$tmnxNatNotifyDescription$*
Cause	The tmnxNatInAddrPrefixBlksFree notification is sent when all port blocks allocated to one or more subscribers associated with a particular set of inside addresses are released by this system. The type of subscriber(s) is indicated by tmnxNatNotifySubscriberType. The set of inside IP addresses is associated with the virtual router instance indicated by tmnxNatNotifyInsideVRtrID and is of the type indicated by tmnxNatNotifyInsideAddrType. The set of inside IP addresses consists of the address prefix indicated with tmnxNatNotifyInsideAddr and tmnxNatNotifyInsideAddrPrefixLen unless these objects are empty and zero; if tmnxNatNotifyInsideAddr is empty and tmnxNatNotifyInsideAddrPrefixLen is zero, the set contains all IP addresses of the indicated type. The values of tmnxNatNotifyMdaChassisIndex, tmnxNatNotifyMdaCardSlotNum and tmnxNatNotifyMdaSlotNum identify the ISA MDA where the blocks were processed. All notifications of this type are sequentially numbered with the tmnxNatNotifyPlSeqNum. This type of

Property name	Value
	notification is typically the consequence of one or more configuration changes; the nature of these changes is indicated in the tmnxNatNotify Description.
Effect	N/A
Recovery	N/A

47.7 tmnxNatIsaGrpIsDegraded

Table 830: tmnxNatIsaGrpIsDegraded properties

Property name	Value
Application name	NAT
Event ID	2025
Event name	tmnxNatIsaGrpIsDegraded
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.25
Default severity	minor
Message format string	The NAT group *$tmnxNatIsaGrpId$* is *$tmnxNatIsaGrpDegraded$*.
Cause	The tmnxNatIsaGrpIsDegraded notification is sent when the value of the object tmnxNatIsaGrpDegraded changes.
Effect	N/A
Recovery	N/A

47.8 tmnxNatIsaGrpOperStateChanged

Table 831: tmnxNatIsaGrpOperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2024
Event name	tmnxNatIsaGrpOperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.24

Property name	Value
Default severity	minor
Message format string	The state of NAT group *$tmnxNatIsaGrpId$* changed to *$tmnxNatIsaGrpOperState$*.
Cause	The tmnxNatIsaGrpOperStateChanged notification is sent when the value of the object tmnxNatIsaGrpOperState changes.
Effect	N/A
Recovery	N/A

47.9 tmnxNatIsaMemberSessionUsageHigh

Table 832: tmnxNatIsaMemberSessionUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2002
Event name	tmnxNatIsaMemberSessionUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.2
Default severity	warning
Message format string	The session usage high water status changed to *$tmnxNatIsaMemberSessionUsageHi$*.
Cause	N/A
Effect	N/A
Recovery	N/A

47.10 tmnxNatL2AwSubIcmpPortUsageHigh

Table 833: tmnxNatL2AwSubIcmpPortUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2007

Property name	Value
Event name	tmnxNatL2AwSubIcmpPortUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.7
Default severity	warning
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

47.11 tmnxNatL2AwSubSessionUsageHigh

Table 834: tmnxNatL2AwSubSessionUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2010
Event name	tmnxNatL2AwSubSessionUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.10
Default severity	warning
Message format string	The session usage high water status changed to *$tmnxNatL2AwSub StatSessionUsageHi$*.
Cause	N/A
Effect	N/A
Recovery	N/A

47.12 tmnxNatL2AwSubTcpPortUsageHigh

Table 835: tmnxNatL2AwSubTcpPortUsageHigh properties

Property name	Value
Application name	NAT

Property name	Value
Event ID	2009
Event name	tmnxNatL2AwSubTcpPortUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.9
Default severity	warning
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

47.13 tmnxNatL2AwSubUdpPortUsageHigh

Table 836: tmnxNatL2AwSubUdpPortUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2008
Event name	tmnxNatL2AwSubUdpPortUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.8
Default severity	warning
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

47.14 tmnxNatLsnSubBlksFree

Table 837: tmnxNatLsnSubBlksFree properties

Property name	Value
Application name	NAT

Property name	Value
Event ID	2021
Event name	tmnxNatLsnSubBlksFree
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.21
Default severity	minor
Message format string	{*$tmnxNatNotifyPlSeqNum$*} LSN subscriber all blocks freed *$tmnxNatNotifyLsnSubId$ $tmnxNatNotifySubscriberType$* %*$tmnxNatNotifyNumber$ $tmnxNatNotifyInsideVRtrID$ $tmnxNatNotifyInsideAddr$* MDA *$tmnxNatNotifyMdaCardSlotNum$*/*$tmnxNatNotifyMdaSlotNum$* at *$tmnxNatNotifyDateAndTime$*
Cause	The tmnxNatLsnSubBlksFree notification is sent when all port blocks allocated to a Large Scale NAT (LSN) subscriber are released. The NAT subscriber is identified with its subscriber ID tmnxNatNotifyLsnSubId. To further facilitate the identification of the NAT subscriber, its type tmnxNatNotifySubscriberType, inside IP address tmnxNatNotifyInsideAddr and inside virtual router instance tmnxNatNotifyInsideVRtrID are provided. The values of tmnxNatNotifyMdaChassisIndex, tmnxNatNotifyMdaCardSlotNum and tmnxNatNotifyMdaSlotNum identify the ISA MDA where the blocks were processed. All notifications of this type are sequentially numbered with the tmnxNatNotifyPlSeqNum.
Effect	N/A
Recovery	N/A

47.15 tmnxNatLsnSubIcmpPortUsgHigh

Table 838: tmnxNatLsnSubIcmpPortUsgHigh properties

Property name	Value
Application name	NAT
Event ID	2026
Event name	tmnxNatLsnSubIcmpPortUsgHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.26
Default severity	warning
Message format string	The ICMP port usage high water status changed to *$tmnxNatQryLsnSubResIcmpPortUsgHi$* for host *$tmnxNatNotifyInsideAddr$* in router *$tmnxNatNotifyInsideVRtrID$* policy

Property name	Value
Cause	The tmnxNatLsnSubIcmpPortUsgHigh notification is sent when the ICMP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false'). If only a single host can be associated with this subscriber, it is identified with its inside IP address tmnxNatNotifyInsideAddr in the inside virtual router instance tmnxNatNotifyInsideVRtrID; otherwise, these objects contain null values.
Effect	N/A
Recovery	N/A

47.16 tmnxNatLsnSubSessionUsgHigh

Table 839: tmnxNatLsnSubSessionUsgHigh properties

Property name	Value
Application name	NAT
Event ID	2029
Event name	tmnxNatLsnSubSessionUsgHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.29
Default severity	warning
Message format string	The session usage high water status changed to *$tmnxNatQryLsnSubResSessionUsgHi$* for host *$tmnxNatNotifyInsideAddr$* in router *$tmnxNatNotifyInsideVRtrID$* policy
Cause	The tmnxNatLsnSubSessionUsgHigh notification is sent when the session usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false'). If only a single host can be associated with this subscriber, it is identified with its inside IP address tmnxNatNotifyInsideAddr in the inside virtual router instance tmnxNatNotifyInsideVRtrID; otherwise, these objects contain null values.
Effect	N/A
Recovery	N/A

47.17 tmnxNatLsnSubTcpPortUsgHigh

Table 840: tmnxNatLsnSubTcpPortUsgHigh properties

Property name	Value
Application name	NAT
Event ID	2028
Event name	tmnxNatLsnSubTcpPortUsgHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.28
Default severity	warning
Message format string	The TCP port usage high water status changed to *$tmnxNatQryLsnSubResTcpPortUsgHi$* for host *$tmnxNatNotifyInsideAddr$* in router *$tmnxNatNotifyInsideVRtrID$* policy
Cause	The tmnxNatLsnSubTcpPortUsgHigh notification is sent when the TCP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false'). If only a single host can be associated with this subscriber, it is identified with its inside IP address tmnxNatNotifyInsideAddr in the inside virtual router instance tmnxNatNotifyInsideVRtrID; otherwise, these objects contain null values.
Effect	N/A
Recovery	N/A

47.18 tmnxNatLsnSubUdpPortUsgHigh

Table 841: tmnxNatLsnSubUdpPortUsgHigh properties

Property name	Value
Application name	NAT
Event ID	2027
Event name	tmnxNatLsnSubUdpPortUsgHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.27
Default severity	warning
Message format string	The UDP port usage high water status changed to *$tmnxNatQryLsnSubResUdpPortUsgHi$* for host *$tmnxNatNotifyInsideAddr$* in router *$tmnxNatNotifyInsideVRtrID$* policy

Property name	Value
Cause	The tmnxNatLsnSubUdpPortUsgHigh notification is sent when the UDP port usage of a Large Scale NAT subscriber reaches its high watermark ('true') or when it reaches its low watermark again ('false'). If only a single host can be associated with this subscriber, it is identified with its inside IP address tmnxNatNotifyInsideAddr in the inside virtual router instance tmnxNatNotifyInsideVRtrID; otherwise, these objects contain null values.
Effect	N/A
Recovery	N/A

47.19 tmnxNatMapRuleChange

Table 842: tmnxNatMapRuleChange properties

Property name	Value
Application name	NAT
Event ID	2036
Event name	tmnxNatMapRuleChange
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.36
Default severity	minor
Message format string	map-t map-domain *$tmnxNatMapDomName$* mapping-rule *$tmnxNatMapRuleName$* rule-prefix= *$tmnxNatMapRulePrefix$*/*$tmnxNatMapRulePrefixLength$* ipv4-prefix= *$tmnxNatMapRuleIpv4Prefix$*/*$tmnxNatMapRuleIpv4PrefixLength$* ea-length= *$tmnxNatMapRuleEaLength$* psid-offset=*$tmnxNatMapRulePsidOffset$* *$tmnxNatNotifyTruthValue$* in router *$vRtrID$* at *$tmnxNatNotifyDateAndTime$*
Cause	The tmnxNatMapRuleChange notification is sent with the value 'true' for tmnxNatNotifyTruthValue when a mapping rule becomes operational. The same notification is sent with 'false' when a mapping rule ceases to be operational. The value of the vRtrID object indicates in what virtual router instance the system applied the rule. The value of the tmnxNatNotifyDateAndTime object indicates at what time the system performed the change.
Effect	The system applies a given mapping rule in the time interval between the time it sends the notification with 'true' and the time it sent the notification with 'false'.
Recovery	Not required.

47.20 tmnxNatMdaActive

Table 843: tmnxNatMdaActive properties

Property name	Value
Application name	NAT
Event ID	2020
Event name	tmnxNatMdaActive
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.20
Default severity	minor
Message format string	The NAT MDA *$tmnxCardSlotNum$*/ *$tmnxMDASlotNum$* is now *$tmnxNatNotifyTruthValue$* in group *$tmnxNatIsaGrpId$* .
Cause	The tmnxNatMdaActive notification is sent when the value of the object tmnxNatIsaMdaStatOperState changes from 'primary' to any other value, or the other way around. The value 'primary' means that the MDA is active in the group.
Effect	N/A
Recovery	N/A

47.21 tmnxNatMdaDetectsLoadSharingErr

Table 844: tmnxNatMdaDetectsLoadSharingErr properties

Property name	Value
Application name	NAT
Event ID	2023
Event name	tmnxNatMdaDetectsLoadSharingErr
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.23
Default severity	minor
Message format string	The NAT MDA *$tmnxCardSlotNum$*/ *$tmnxMDASlotNum$* in group *$tmnxNatIsaGrpId$* has detected load sharing errors and has dropped *$tmnxNatNotifyCounter$* more packets.

Property name	Value
Cause	The ingress IOM hardware does not support a particular NAT function's load-balancing, for example an IOM-2 does not support deterministic NAT.
Effect	The MDA drops all incorrectly load-balanced traffic.
Recovery	Upgrade the ingress IOM, or change the configuration.

47.22 tmnxNatPcpSrvStateChanged

Table 845: tmnxNatPcpSrvStateChanged properties

Property name	Value
Application name	NAT
Event ID	2018
Event name	tmnxNatPcpSrvStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.18
Default severity	minor
Message format string	The state of server *$tmnxNatPcpSrvName$* changed to *$tmnxNatPcp SrvState$ - $tmnxNatPcpSrvStateDescription$*
Cause	The tmnxNatPcpSrvStateChanged notification is sent when the value of the object tmnxNatPcpSrvState changes. The cause is explained in the tmnxNatPcpSrvStateDescription.
Effect	While the value of the object tmnxNatPcpSrvState is equal to 'out OfService', the system drops PCP requests addressed to this server.
Recovery	The recovery action depends on the actual cause as specified in the tmnxNatPcpSrvStateDescription.

47.23 tmnxNatPlAddrFree

Table 846: tmnxNatPlAddrFree properties

Property name	Value
Application name	NAT
Event ID	2016

Property name	Value
Event name	tmnxNatPlAddrFree
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.16
Default severity	minor
Message format string	TODO
Cause	The tmnxNatPlAddrFree notification is sent when a range of outside IP addresses becomes free at once. The range starts at address tmnx NatNotifyOutsideAddr and ends with address tmnxNatNotifyOutside EndAddr. It replaces a number of tmnxNatPlBlockAllocationL2Aw or tmnxNatPlBlockAllocationLsn notifications; the allocated port blocks associated with each IP address in the indicated range are released. The reason why this address range is released, is described in the tmnxNatNotifyDescription. If the value of tmnxNatNotifyInsideVRtrID is not equal to zero, it means that only the port blocks associated with hosts in that particular virtual router instance are released; if the value of tmnxNatNotifyInsideVRtrID is equal to zero, it means that all the port blocks are released.
Effect	N/A
Recovery	N/A

47.24 tmnxNatPlBlockAllocationL2Aw

Table 847: tmnxNatPlBlockAllocationL2Aw properties

Property name	Value
Application name	NAT
Event ID	2013
Event name	tmnxNatPlBlockAllocationL2Aw
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.13
Default severity	minor
Message format string	{*$tmnxNatNotifyPlSeqNum$*} *$tmnxNatNotifyTruthValue$ $tmnxNat NotifyOutsideAddr$* [*$tmnxNatNotifyPort$- $tmnxNatNotifyPort2$*] -- l2-aware-sub *$tmnxNatNotifyL2AwSubIdent$* policy *$tmnxNatNotifyName $ $tmnxNatNotifyInsideAddr$* at *$tmnxNatNotifyDateAndTime$*
Cause	The tmnxNatPlBlockAllocationL2Aw notification is sent when an outside IP address and a range of ports is allocated to a NAT subscriber associated with a Layer-2-Aware NAT pool, and when this allocation

Property name	Value
	expires. The allocated block is within the scope of the outside virtual router instance tmnxNatNotifyOutsideVRtrID and the outside IP address tmnxNatNotifyOutsideAddr; it starts with port tmnxNatNotify Port and ends with port tmnxNatNotifyPort2. The NAT subscriber is identified with its subscriber ID tmnxNatNotifyL2AwSubIdent. The NAT policy is identified with its name tmnxNatNotifyName. When the block allocation is made, the value of the object tmnxNatNotifyTruthValue is 'true'; when the block allocation expires, it is 'false'.
Effect	N/A
Recovery	N/A

47.25 tmnxNatPlBlockAllocationLsn

Table 848: tmnxNatPlBlockAllocationLsn properties

Property name	Value
Application name	NAT
Event ID	2012
Event name	tmnxNatPlBlockAllocationLsn
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.12
Default severity	minor
Message format string	TODO
Cause	The tmnxNatPlBlockAllocationLsn notification is sent when an outside IP address and a range of ports is allocated to a NAT subscriber associated with a Large Scale NAT (LSN) pool, and when this allocation expires. The allocated block is within the scope of the outside virtual router instance tmnxNatNotifyOutsideVRtrID and the outside IP address tmnxNatNotifyOutsideAddr; it starts with port tmnxNatNotify Port and ends with port tmnxNatNotifyPort2. The NAT subscriber is identified with its subscriber ID tmnxNatNotifyLsnSubId. To further facilitate the identification of the NAT subscriber, its type tmnxNatNotify SubscriberType, inside IP address tmnxNatNotifyInsideAddr and inside virtual router instance tmnxNatNotifyInsideVRtrID are provided. The values of tmnxNatNotifyMdaChassisIndex, tmnxNatNotifyMdaCard SlotNum and tmnxNatNotifyMdaSlotNum identify the ISA MDA where this block is processed. The value of tmnxNatNotifyNumber is the numerical identifier of the NAT policy used for this allocation; it can be used for correlation of notifications, especially with the tmnxNat PlAddrFree summary event, that may indicate this number in the tmnx NatNotifyDescription object. When the block allocation is made, the

Property name	Value
	value of the object tmnxNatNotifyTruthValue is 'true'; when the block allocation expires, it is 'false'.
Effect	N/A
Recovery	N/A

47.26 tmnxNatPlL2AwBlockUsageHigh

Table 849: tmnxNatPlL2AwBlockUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2001
Event name	tmnxNatPlL2AwBlockUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.1
Default severity	warning
Message format string	The block usage high water status changed to *$tmnxNatPlBlockUsageHi$*.
Cause	N/A
Effect	N/A
Recovery	N/A

47.27 tmnxNatPlLsnMemberBlockUsageHigh

Table 850: tmnxNatPlLsnMemberBlockUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2003
Event name	tmnxNatPlLsnMemberBlockUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.3
Default severity	warning

Property name	Value
Message format string	TODO
Cause	N/A
Effect	N/A
Recovery	N/A

47.28 tmnxNatPlLsnRedActiveChanged

Table 851: tmnxNatPlLsnRedActiveChanged properties

Property name	Value
Application name	NAT
Event ID	2017
Event name	tmnxNatPlLsnRedActiveChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.17
Default severity	warning
Message format string	TODO
Cause	The tmnxNatPlLsnRedActiveChanged notification is sent when the value of the object tmnxNatPlLsnRedActive changes. The cause is explained in the tmnxNatNotifyDescription.
Effect	While the value of the object tmnxNatPlLsnRedActive is equal to 'false', ... - this system is not performing Large Scale NAT in the realm of the virtual router instance associated with this pool; the Large Scale NAT is supposed to be performed by its redundant peer. - the route specified with tmnxNatVrtrInRedSteerRt is not advertised in the realm of any inside virtual router instance associated with this pool; - NAT traffic matching a filter with TFilterAction equal to 'nat' is redirected to the address specified with tmnxNatVrtrInRedPeerAddr or dropped if tmnxNatVrtrInRedPeerAddr is not configured; - the pool ranges associated with this pool are withdrawn from the outside virtual router instance associated with this pool; - the route specified with tmnxNat PlLsnRedExpPrefix is not exported in the realm of the outside virtual router instance associated with this pool.
Recovery	If this system is supposed to assume the role of a standby in the realm of the virtual router instance associated with this pool, no recovery is needed. Otherwise, the recovery action will depend on the actual cause as specified in the tmnxNatNotifyDescription.

47.29 tmnxNatResourceProblemCause

Table 852: tmnxNatResourceProblemCause properties

Property name	Value
Application name	NAT
Event ID	2015
Event name	tmnxNatResourceProblemCause
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.15
Default severity	minor
Message format string	*$tmnxNatNotifyDescription$*
Cause	N/A
Effect	N/A
Recovery	N/A

47.30 tmnxNatResourceProblemDetected

Table 853: tmnxNatResourceProblemDetected properties

Property name	Value
Application name	NAT
Event ID	2014
Event name	tmnxNatResourceProblemDetected
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.14
Default severity	minor
Message format string	The status of the NAT resource problem indication changed to *$tmnx NatResourceProblem$*.
Cause	N/A
Effect	N/A
Recovery	N/A

47.31 tmnxNatVrtrOutDnatOnlyRoutesHigh

Table 854: tmnxNatVrtrOutDnatOnlyRoutesHigh properties

Property name	Value
Application name	NAT
Event ID	2035
Event name	tmnxNatVrtrOutDnatOnlyRoutesHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.35
Default severity	warning
Message format string	The DNAT-only routes high water status changed to *$tmnxNatNotifyTruthValue$*: *$tmnxNatVrtrOutDnatOnlyRoutes$*/ *$tmnxNatVrtrOutDnatOnlyRouteLimit$*.
Cause	The tmnxNatVrtrOutDnatOnlyRoutesHigh notification is sent with the value 'true' for tmnxNatNotifyTruthValue when the actual value of the object tmnxNatVrtrOutDnatOnlyRoutes approaches the configured value of tmnxNatVrtrOutDnatOnlyRouteLimit for a given virtual router instance. The same notification is sent with 'false' for tmnxNatNotifyTruthValue when the value of tmnxNatVrtrOutDnatOnlyRoutes goes below the threshold value again.
Effect	While the value of tmnxNatVrtrOutDnatOnlyRoutes is between the threshold value and the tmnxNatVrtrOutDnatOnlyRouteLimit limit, there is no effect. When an attempt is made to change the configuration within the virtual router instance such that the actual value of tmnxNatVrtrOutDnatOnlyRoutes would exceed the tmnxNatVrtrOutDnatOnlyRouteLimit limit, the system would refuse that attempt.
Recovery	Within the associated NAT inside virtual router instance, - reduce the number of prefixes (in the tmnxNatPrefixTable), - reduce the value of tmnxNatVrtrInMaxDetSubscrLimit.

48 NTP

48.1 tmnxNtpAuthMismatch

Table 855: tmnxNtpAuthMismatch properties

Property name	Value
Application name	NTP
Event ID	2001
Event name	tmnxNtpAuthMismatch
SNMP notification prefix and OID	TIMETRA-NTP-MIB.tmnxNtpNotifications.1
Default severity	warning
Message format string	NTP message is received with an *$tmnxNtpAuthKeyFailType$* from *$tmnxNtpPeersPeerAddress$*
Cause	The managed object tmnxNtpAuthCheck has a value of true and an NTP message was received with an incorrect authentication key or type.
Effect	N/A
Recovery	N/A

48.2 tmnxNtpNoServersAvail

Table 856: tmnxNtpNoServersAvail properties

Property name	Value
Application name	NTP
Event ID	2002
Event name	tmnxNtpNoServersAvail
SNMP notification prefix and OID	TIMETRA-NTP-MIB.tmnxNtpNotifications.2
Default severity	major
Message format string	No NTP servers are available.

Property name	Value
Cause	No NTP servers are available.
Effect	N/A
Recovery	N/A

48.3 tmnxNtpOperChange

Table 857: tmnxNtpOperChange properties

Property name	Value
Application name	NTP
Event ID	2008
Event name	tmnxNtpOperChange
SNMP notification prefix and OID	TIMETRA-NTP-MIB.tmnxNtpNotifications.7
Default severity	warning
Message format string	NTP's operational status is *$tmnxNtpOperState$*
Cause	There has been a change in the operational state of NTP.
Effect	N/A
Recovery	N/A

48.4 tmnxNtpServerChange

Table 858: tmnxNtpServerChange properties

Property name	Value
Application name	NTP
Event ID	2009
Event name	tmnxNtpServerChange
SNMP notification prefix and OID	TIMETRA-NTP-MIB.tmnxNtpNotifications.8
Default severity	minor

Property name	Value
Message format string	NTP server has changed: Old server *$strOldServer$*, New server *$tmnxNtpPeersPeerAddress$*
Cause	More than one NTP servers are configured in a system and a different NTP server has been selected because the operational status of the earlier NTP server has changed.
Effect	A new NTP server was selected.
Recovery	N/A

48.5 tmnxNtpServersAvail

Table 859: tmnxNtpServersAvail properties

Property name	Value
Application name	NTP
Event ID	2003
Event name	tmnxNtpServersAvail
SNMP notification prefix and OID	TIMETRA-NTP-MIB.tmnxNtpNotifications.3
Default severity	minor
Message format string	NTP servers are available.
Cause	NTP servers are now available.
Effect	N/A
Recovery	N/A

49 OAM

49.1 aluTwampReflnactivityTimeout

Table 860: aluTwampReflnactivityTimeout properties

Property name	Value
Application name	OAM
Event ID	2300
Event name	aluTwampReflnactivityTimeout
SNMP notification prefix and OID	ALU-VRTR-MIB.aluTwampNotifications.1
Default severity	minor
Message format string	TODO
Cause	The aluTwampReflnactivityTimeout notification is generated when a TWAMP test session was disconnected by the TWAMP Reflector because the session was inactive for a period exceeding the reflector's inactivity timeout (aluTwampRefInactTimeout).
Effect	The TWAMP reflector cannot receive any traffic on the disconnected session.
Recovery	Check the IP connectivity between this reflector and the TWAMP client.

49.2 svcIdInvalid

Table 861: svcIdInvalid properties

Property name	Value
Application name	OAM
Event ID	2053
Event name	svcIdInvalid
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Message format string	Service id *$serviceId$* is invalid: *$reasonToReport$*
Cause	Svc-ping tried to send or process a packet to a non-existent svc-id.
Effect	N/A
Recovery	N/A

49.3 svcIdWrongType

Table 862: svcIdWrongType properties

Property name	Value
Application name	OAM
Event ID	2054
Event name	svcIdWrongType
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Service id *$serviceId$* has a wrong type: *$reasonToReport$*
Cause	Svc-ping tried to send or process a packet to a svc-id with a wrong svc-type.
Effect	N/A
Recovery	N/A

49.4 tmnxAncpLoopbackTestCompleted

Table 863: tmnxAncpLoopbackTestCompleted properties

Property name	Value
Application name	OAM
Event ID	2004
Event name	tmnxAncpLoopbackTestCompleted
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamPingNotifications.7

Property name	Value
Default severity	warning
Message format string	The ANCP loopback test for ANCP string *$tmnxOamAncpHistoryAncpString$* has ended. The access Node has sent Result *$tmnxOamAncpHistoryAccNodeResult$*; code*$tmnxOamAncpHistoryAccNodeCode$*; and reply string *$tmnxOamAncpHistoryAccNodeRspStr$*.
Cause	An ANCP loopback is finished and a notification was explictly requested.
Effect	N/A
Recovery	N/A

49.5 tmnxAncpLoopbackTestCompletedL

Table 864: tmnxAncpLoopbackTestCompletedL properties

Property name	Value
Application name	OAM
Event ID	2005
Event name	tmnxAncpLoopbackTestCompletedL
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	The ANCP loopback test for ANCP string *$tmnxOamAncpHistoryAncpString$* has ended. The access Node has sent Result *$tmnxOamAncpHistoryAccNodeResult$*; code*$tmnxOamAncpHistoryAccNodeCode$*; and reply string *$tmnxOamAncpHistoryAccNodeRspStr$*.
Cause	N/A
Effect	N/A
Recovery	N/A

49.6 tmnxOamLdpTtraceAutoDiscState

Table 865: tmnxOamLdpTtraceAutoDiscState properties

Property name	Value
Application name	OAM
Event ID	2055
Event name	tmnxOamLdpTtraceAutoDiscState
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.4
Default severity	minor
Message format string	The discovery state of the 'Auto Ldp Tree Trace entity' has changed to *$tmnxOamLTtraceAutoDiscoveryState$*
Cause	The discovery state of the 'Auto Ldp Tree Trace entity' represented by tmnxOamLTtraceAutoDiscoveryState has been changed.
Effect	N/A
Recovery	N/A

49.7 tmnxOamLdpTtraceFecDisStatus

Table 866: tmnxOamLdpTtraceFecDisStatus properties

Property name	Value
Application name	OAM
Event ID	2057
Event name	tmnxOamLdpTtraceFecDisStatus
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.6
Default severity	minor
Message format string	The FEC *$strTmnxOamLTtraceFecPrefix$*/ *$strTmnxOamLTtraceFec PrefLen$* is discovered with *$tmnxOamLTtraceFecDisPaths$* paths. The discovery status BITs are *$strTmnxOamLTtraceFecDisStatusBits$*.
Cause	The discovery status BITS or the number of discovered paths of the 'auto discovered FEC' has been changed. Note that the changes were evaluated at the end of a FEC discovery.
Effect	N/A

Property name	Value
Recovery	N/A

49.8 tmnxOamLdpTtraceFecPFailUpdate

Table 867: tmnxOamLdpTtraceFecPFailUpdate properties

Property name	Value
Application name	OAM
Event ID	2058
Event name	tmnxOamLdpTtraceFecPFailUpdate
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.7
Default severity	minor
Message format string	Path probe state update for the 'auto discovered' FEC, *$strTmnx OamLTtraceFecPrefix$*/*$strTmnxOamLTtraceFecPrefLen$*. *$tmnx OamLTtraceFecFailedProbes$* out of *$tmnxOamLTtraceFecDisPaths$* paths are in failed probing state.
Cause	The probe state of the 'auto discovered FEC' has been changed.
Effect	N/A
Recovery	N/A

49.9 tmnxOamLdpTtraceFecProbeState

Table 868: tmnxOamLdpTtraceFecProbeState properties

Property name	Value
Application name	OAM
Event ID	2056
Event name	tmnxOamLdpTtraceFecProbeState
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.5
Default severity	minor
Message format string	The probe state of the 'auto discovered' FEC, *$strTmnxOamLTtrace FecPrefix$*/*$strTmnxOamLTtraceFecPrefLen$*, has changed to *$tmnx*

Property name	Value
	OamLTtraceFecProbeState$.$tmnxOamLTtraceFecFailedProbes$* out of *$tmnxOamLTtraceFecDisPaths$ paths are in failed probing state.
Cause	The probe state of the 'auto discovered FEC' has been changed.
Effect	N/A
Recovery	N/A

49.10 tmnxOamPingProbeFailedV3

Table 869: tmnxOamPingProbeFailedV3 properties

Property name	Value
Application name	OAM
Event ID	2001
Event name	tmnxOamPingProbeFailedV3
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamPingNotifications.8
Default severity	minor
Message format string	OAM *$tmnxOamPingCtlTestMode$* test " *$tmnxOamPingCtlTestIndex $*" created by "*$tmnxOamPingCtlOwnerIndex$*" run # *$tmnxOamPing ResultsTestRunIndex$* probe *$tmnxOamPingHistoryIndex$* failed
Cause	A probe failure was detected when the corresponding tmnxOamPing CtlTrapGeneration object is set to probeFailure(0) subject to the value of tmnxOamPingCtlTrapProbeFailureFilter. The object tmnxOam PingCtlTrapProbeFailureFilter can be used to specify the number of successive probe failures that are required before this notification can be generated.
Effect	N/A
Recovery	N/A

49.11 tmnxOamPingTestCompletedV3

Table 870: tmnxOamPingTestCompletedV3 properties

Property name	Value
Application name	OAM

Property name	Value
Event ID	2003
Event name	tmnxOamPingTestCompletedV3
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamPingNotifications.10
Default severity	minor
Message format string	OAM *$tmnxOamPingCtlTestMode$* test " *$tmnxOamPingCtlTestIndex $*" created by "*$tmnxOamPingCtlOwnerIndex$*" run # *$tmnxOamPing ResultsTestRunIndex$* completed
Cause	A ping test when the corresponding tmnxOamPingCtlTrapGeneration object is set to testCompletion(2).
Effect	N/A
Recovery	N/A

49.12 tmnxOamPingTestFailedV3

Table 871: tmnxOamPingTestFailedV3 properties

Property name	Value
Application name	OAM
Event ID	2002
Event name	tmnxOamPingTestFailedV3
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamPingNotifications.9
Default severity	minor
Message format string	OAM *$tmnxOamPingCtlTestMode$* test " *$tmnxOamPingCtlTestIndex $*" created by "*$tmnxOamPingCtlOwnerIndex$*" run # *$tmnxOamPing ResultsTestRunIndex$* failed
Cause	A ping test failed when the corresponding tmnxOamPingCtlTrap Generation object is set to testFailure(1). In this instance tmnxOam PingCtlTrapTestFailureFilter specifies the number of probes in a test required to have failed in order to consider the test as failed.
Effect	N/A
Recovery	N/A

49.13 tmnxOamPmThrClear

Table 872: tmnxOamPmThrClear properties

Property name	Value
Application name	OAM
Event ID	2301
Event name	tmnxOamPmThrClear
SNMP notification prefix and OID	TIMETRA-OAM-PM-MIB.tmnxOamPmNotifications.2
Default severity	warning
Message format string	OAM-PM TCA cleared for session " *$tmnxOamPmCfgSessName$*", test type *$tmnxOamPmStsBaseTestType$*, measurement interval duration *$tmnxOamPmStsMeasIntvlDuration$*, MI start *$tmnxOam PmStsBaseStartTime$* UTC, delay bin type *$tmnxOamPmNotifThr DelayBinType$*. Threshold type *$tmnxOamPmNotifThrType$*, direction *$tmnxOamPmNotifThrDirection$*, bin lower bound (us) *$tmnxOam PmNotifThrBinLowerBound$*, configured threshold *$tmnxOamPmNotif ThrCfgClear$*, operational value *$tmnxOamPmNotifThrOperClear$*. TCA type *$tmnxOamPmNotifThrStateType$*, suspect flag *$tmnxOam PmStsBaseSuspect$*.
Cause	A tmnxOamPmThrClear trap is sent at the end of an OAM-PM measurement interval when a loss or delay counter meets or falls below its configured Clear threshold. At most one tmnxOamPmThr Clear trap is sent per tmnxOamPmThrRaise trap. OAM-PM thresholds are explained in the description clauses of tmnxOamPmCfgThrDelay Table, tmnxOamPmCfgThrLossFwBwAgTable, and tmnxOamPmCfg ThrLossFwBwTable. OAM-PM counters are explained in the description clauses of the tmnxOamPmStatsTableObjs tables.
Effect	For an LMM test, the loss of live traffic has met or fallen below a configured threshold. For other test types, the loss or delay of OAM-PM test probes has met or fallen below a configured threshold, indicating a possible improvement in the loss or delay of live traffic.
Recovery	No recovery is required for this trap.

49.14 tmnxOamPmThrRaise

Table 873: tmnxOamPmThrRaise properties

Property name	Value
Application name	OAM

Property name	Value
Event ID	2300
Event name	tmnxOamPmThrRaise
SNMP notification prefix and OID	TIMETRA-OAM-PM-MIB.tmnxOamPmNotifications.1
Default severity	warning
Message format string	OAM-PM TCA raised for session " *$tmnxOamPmCfgSessName$*", test type *$tmnxOamPmStsBaseTestType$*, measurement interval duration *$tmnxOamPmStsMeasIntvlDuration$*, MI start *$tmnxOamPmStsBase StartTime$* UTC, delay bin type *$tmnxOamPmNotifThrDelayBinType $*. Threshold type *$tmnxOamPmNotifThrType$*, direction *$tmnxOam PmNotifThrDirection$*, bin lower bound (us) *$tmnxOamPmNotifThrBin LowerBound$*, configured threshold *$tmnxOamPmNotifThrCfgRaise $*, operational value *$tmnxOamPmNotifThrOperRaise$*. TCA type *$tmnxOamPmNotifThrStateType$*, suspect flag *$tmnxOamPmStsBase Suspect$*.
Cause	A tmnxOamPmThrRaise trap is sent when an OAM-PM loss or delay counter meets or exceeds its configured Raise threshold. If an Average Frame Loss Ratio (FLR) threshold (i.e. tmnxOamPmCfgThrLossAvg FlrRaise) is met or exceeded, the tmnxOamPmThrRaise trap is sent at the end of the measurement interval. If another type of threshold (e.g. tmnxOamPmCfgThrLossHliRaise) is met or exceeded, the tmnx OamPmThrRaise trap is sent when the problem is detected. The Average FLR threshold is a special case because the measured Average FLR can fluctuate during a measurement interval. At most one tmnxOamPmThrRaise trap is sent per threshold type during one OAM-PM measurement interval. For example, at most one tmnxOam PmThrRaise trap is sent to record an excessive High Loss Indicator (HLI) count in the forward direction seen in a particular 15 minute interval belonging to the SLM test belonging to OAM-PM session 'oam PmSession1'. OAM-PM thresholds are explained in the description clauses of tmnxOamPmCfgThrDelayTable, tmnxOamPmCfgThrLoss FwBwAgTable, and tmnxOamPmCfgThrLossFwBwTable. OAM-PM counters are explained in the description clauses of the tmnxOam PmStatsTableObjs tables.
Effect	For an LMM test, the loss of live traffic has met or exceeded a configured threshold. For the other test types, the loss or delay of OAM-PM test probes has met or exceeded a configured threshold, indicating possible excessive loss or excessive delay of live traffic.
Recovery	Fix the cause of the excessive loss or excessive delay.

49.15 tmnxOamSaaThreshold

Table 874: tmnxOamSaaThreshold properties

Property name	Value
Application name	OAM
Event ID	2101
Event name	tmnxOamSaaThreshold
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamSaaNotifications.1
Default severity	minor
Message format string	OAM SAA *$tmnxOamSaaCtlTestMode$* test " *$tmnxOamSaaCtlTestIndex$*" created by "*$tmnxOamSaaCtlOwnerIndex$*" run # *$tmnxOamSaaTTestRunIndex$* crossed *$tmnxOamSaaTDirection$ $tmnxOamSaaTType$* threshold *$tmnxOamSaaTThreshold$* with value *$tmnxOamSaaTValue$*
Cause	At the completion of an SAA OAM trace route test the threshold has been crossed for a results statistic.
Effect	N/A
Recovery	N/A

49.16 tmnxOamTrPathChange

Table 875: tmnxOamTrPathChange properties

Property name	Value
Application name	OAM
Event ID	2050
Event name	tmnxOamTrPathChange
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.1
Default severity	minor
Message format string	OAM *$tmnxOamTrCtlTestMode$* test " *$tmnxOamTrCtlTestIndex$*" created by "*$tmnxOamTrCtlOwnerIndex$*" run # *$tmnxOamTrResultsTestRunIndex$* path changed
Cause	The path to a target has changed.
Effect	N/A

Property name	Value
Recovery	N/A

49.17 tmnxOamTrTestCompleted

Table 876: tmnxOamTrTestCompleted properties

Property name	Value
Application name	OAM
Event ID	2052
Event name	tmnxOamTrTestCompleted
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.3
Default severity	minor
Message format string	OAM *$tmnxOamTrCtlTestMode$* test " *$tmnxOamTrCtlTestIndex$*" created by "*$tmnxOamTrCtlOwnerIndex$*" run # *$tmnxOamTrResults TestRunIndex$* completed
Cause	The OAM trace route test has just completed.
Effect	N/A
Recovery	N/A

49.18 tmnxOamTrTestFailed

Table 877: tmnxOamTrTestFailed properties

Property name	Value
Application name	OAM
Event ID	2051
Event name	tmnxOamTrTestFailed
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamTraceRouteNotifications.2
Default severity	minor
Message format string	OAM *$tmnxOamTrCtlTestMode$* test " *$tmnxOamTrCtlTestIndex$*" created by "*$tmnxOamTrCtlOwnerIndex$*" run # *$tmnxOamTrResults TestRunIndex$* failed

Property name	Value
Cause	The OAM trace route test failed to complete successfully.
Effect	N/A
Recovery	N/A

49.19 tmnxTwampSrvInactivityTimeout

Table 878: tmnxTwampSrvInactivityTimeout properties

Property name	Value
Application name	OAM
Event ID	2200
Event name	tmnxTwampSrvInactivityTimeout
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.1
Default severity	minor
Message format string	TWAMP server control connection to client *$tmnxTwampSrvConnClientAddr$* disconnected because it was inactive for *$tmnxTwampSrvConnIdleTime$* seconds
Cause	The tmnxTwampSrvInactivityTimeout notification is generated when a TWAMP control connection was disconnected by the TWAMP server because the connection was inactive for a period exceeding the server's inactivity timeout (tmnxTwampSrvInactTimeout).
Effect	The TWAMP client cannot request test runs on the disconnected connection.
Recovery	Check the IP connectivity between this node and the TWAMP client.

49.20 tmnxTwampSrvMaxConnsExceeded

Table 879: tmnxTwampSrvMaxConnsExceeded properties

Property name	Value
Application name	OAM
Event ID	2201
Event name	tmnxTwampSrvMaxConnsExceeded

Property name	Value
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.2
Default severity	minor
Message format string	TWAMP server control connection to client *$tmnxTwampSrvNotifClientAddr$* could not be established because the system limit (*$tmnxTwampSrvConnectionCount$* concurrent connections) has been reached
Cause	The tmnxTwampSrvMaxConnsExceeded notification is generated when a TWAMP control connection could not be established by the TWAMP server because the system-level maximum number of concurrent TWAMP control connections (tmnxTwampSrvMaxConnections) has been reached.
Effect	The TWAMP client cannot request test runs on the rejected connection.
Recovery	Configure the system-level maximum number of concurrent TWAMP control connections to a larger value, or disconnect any TWAMP control connection.

49.21 tmnxTwampSrvMaxSessExceeded

Table 880: tmnxTwampSrvMaxSessExceeded properties

Property name	Value
Application name	OAM
Event ID	2203
Event name	tmnxTwampSrvMaxSessExceeded
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.4
Default severity	minor
Message format string	TWAMP server session to client *$tmnxTwampSrvNotifClientAddr$* could not be established because the system limit (*$tmnxTwampSrvSessionCount$* concurrent sessions) has been reached
Cause	The tmnxTwampSrvMaxSessExceeded notification is generated when a TWAMP session could not be established by the TWAMP server because the system-level maximum number of concurrent TWAMP sessions (tmnxTwampSrvMaxSessions) has been reached.
Effect	The TWAMP client cannot request test runs on the rejected session.

Property name	Value
Recovery	Configure the system-level maximum number of concurrent TWAMP sessions to a larger value, or disconnect any TWAMP session.

49.22 tmnxTwampSrvPfxMaxConnsExceeded

Table 881: tmnxTwampSrvPfxMaxConnsExceeded properties

Property name	Value
Application name	OAM
Event ID	2202
Event name	tmnxTwampSrvPfxMaxConnsExceeded
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.3
Default severity	minor
Message format string	TWAMP server control connection to client *$tmnxTwampSrvNotifClient Addr$* could not be established because the limit for prefix *$tmnx TwampSrvPrefixAddr$*/*$tmnxTwampSrvPrefixLen$* (*$tmnxTwampSrv PfxConnCount$* concurrent connections) has been reached
Cause	The tmnxTwampSrvPfxMaxConnsExceeded notification is generated when a TWAMP control connection could not be established by the TWAMP server because the maximum number of concurrent TWAMP control connections configured against the TWAMP client's prefix (tmnx TwampSrvPrefixMaxConnections) has been reached.
Effect	The TWAMP client cannot request test runs on the rejected connection.
Recovery	Configure the prefix's maximum number of concurrent TWAMP control connections to a larger value, or disconnect a TWAMP control connection which uses the prefix.

49.23 tmnxTwampSrvPfxMaxSessExceeded

Table 882: tmnxTwampSrvPfxMaxSessExceeded properties

Property name	Value
Application name	OAM
Event ID	2204

Property name	Value
Event name	tmnxTwampSrvPfxMaxSessExceeded
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.5
Default severity	minor
Message format string	TWAMP server session to client *$tmnxTwampSrvNotifClientAddr$* could not be established because the limit for prefix *$tmnxTwampSrv PrefixAddr$*/*$tmnxTwampSrvPrefixLen$* (*$tmnxTwampSrvPfxSession Count$* concurrent sessions) has been reached
Cause	The tmnxTwampSrvPfxMaxSessExceeded notification is generated when a TWAMP session could not be established by the TWAMP server because the maximum number of concurrent TWAMP sessions configured against the TWAMP client's prefix (tmnxTwampSrvPrefix MaxSessions) has been reached.
Effect	The TWAMP client cannot request test runs on the rejected session.
Recovery	Configure the prefix's maximum number of concurrent TWAMP sessions to a larger value, or disconnect a TWAMP session which uses the prefix.

50 OPEN_FLOW

50.1 tmnxOFFlowEntryInsertFailed

Table 883: tmnxOFFlowEntryInsertFailed properties

Property name	Value
Application name	OPEN_FLOW
Event ID	2001
Event name	tmnxOFFlowEntryInsertFailed
SNMP notification prefix and OID	TIMETRA-OPEN-FLOW-MIB.tmnxOpenFlowNotification.1
Default severity	minor
Message format string	Failed to add flow-entry for open-flow switch " *$tmnxOFSwitch Name$*" flow-table *$tmnxOFFlowTableId$*. Flow-table Oper Status: *$tmnxOFFlowTableOperStatus$*. Failure Reason *$tmnxOFNotify Description$*
Cause	The tmnxOFFlowEntryInsertFailed notification is generated when a flow-entry could not be inserted into an open-flow table.
Effect	The flow-entry won't be available in the flow-table. If inserting of a default flow-entry failed, then the value of tmnxOFFlowTableOperStatus is set to 'outOfService (3)'.
Recovery	In order to insert the failed flow-entry into flow-table is to change the admin state of an open-flow switch instance to 'outOfService (3)' and then back to 'inService (1)' and try inserting the flow-entry again.

51 OSPF

51.1 tmnxOspfAdjBfdSessionSetupFail

Table 884: tmnxOspfAdjBfdSessionSetupFail properties

Property name	Value
Application name	OSPF
Event ID	2057
Event name	tmnxOspfAdjBfdSessionSetupFail
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.57
Default severity	warning
Message format string	BFD session setup failed with reason *$tmnxOspfBfdSessSetupFail Reason$* for Router *$tmnxOspfRouterId$*
Cause	The tmnxOspfAdjBfdSessionSetupFail notification is sent when BFD session setup fails.
Effect	The system can not setup the BFD session.
Recovery	Depending on the tmnxOspfBfdSessSetupFailReason, recovery can be possible. Check the BFD configuration to recover.

51.2 tmnxOspfAreaMaxAgeLsa

Table 885: tmnxOspfAreaMaxAgeLsa properties

Property name	Value
Application name	OSPF
Event ID	2013
Event name	tmnxOspfAreaMaxAgeLsa
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.13
Default severity	warning

Property name	Value
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Max aged LSA *$ospfLsdbLsid$* type *$ospfLsdbType$* area *$ospfLsdbAreaId$* advertising router *$ospf LsdbRtrId$*
Cause	One of the LSA in the router's link-state database has reached its maximum age.
Effect	N/A
Recovery	N/A

51.3 tmnxOspfAreaOriginateLsa

Table 886: tmnxOspfAreaOriginateLsa properties

Property name	Value
Application name	OSPF
Event ID	2012
Event name	tmnxOspfAreaOriginateLsa
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.12
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Originated LSA *$ospfLsdbLsid$* type *$ospfLsdbType$* area *$ospfLsdbAreaId$* advertising router *$ospf LsdbRtrId$*
Cause	A new LSA has been originated by this router. This event is not generated for simple refreshes of LSAs (which happens every 30 minutes), but instead is generated when an LSA is (re)originated due to a topology change. Additionally, this event does not include LSAs that are being flushed because they have reached their maximum age.
Effect	N/A
Recovery	N/A

51.4 tmnxOspfAsMaxAgeLsa

Table 887: tmnxOspfAsMaxAgeLsa properties

Property name	Value
Application name	OSPF
Event ID	2026
Event name	tmnxOspfAsMaxAgeLsa
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.26
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Max aged LSA *$ospfLsdbLsid$* type *$ospfLsdbType$* advertising router *$ospfLsdbRtrId$*
Cause	One of the LSAs in the router's link-state database has reached its maximum age limit.
Effect	N/A
Recovery	N/A

51.5 tmnxOspfAsOriginateLsa

Table 888: tmnxOspfAsOriginateLsa properties

Property name	Value
Application name	OSPF
Event ID	2025
Event name	tmnxOspfAsOriginateLsa
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.25
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Originated LSA *$ospfLsdbLsid$* type *$ospfLsdbType$* advertising router *$ospfLsdbRtrId$*
Cause	A new LSA has been originated by this router. This trap is not generated for simple refreshes of LSAs (which happens every 30 minutes), but instead will only be generated when an LSA is (re)originated due to a topology change. Additionally, this trap does not include LSAs that are being flushed because they have reached their maximum age limit.

Property name	Value
Effect	N/A
Recovery	N/A

51.6 tmnxOspfExportLimitReached

Table 889: tmnxOspfExportLimitReached properties

Property name	Value
Application name	OSPF
Event ID	2039
Event name	tmnxOspfExportLimitReached
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.39
Default severity	major
Message format string	OSPF has reached the export-limit *$tmnxOspfExportLimit$*, additional routes will not be exported into OSPF
Cause	OSPF has exported maximum allowed export routes. It will not export any more routes unless the export policy and export limit is changed.
Effect	OSPF will not export any more routes.
Recovery	Change OSPF export policy.

51.7 tmnxOspfExportLimitWarning

Table 890: tmnxOspfExportLimitWarning properties

Property name	Value
Application name	OSPF
Event ID	2040
Event name	tmnxOspfExportLimitWarning
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.40
Default severity	warning

Property name	Value
Message format string	OSPF has reached *$tmnxOspfExportLimitLogPercent$* percent of the export limit *$tmnxOspfExportLimit$*
Cause	The number of routes exported by OSPF has reached the warning percent of the configured export limit. OSPF will continue to export routes till the limit is reached.
Effect	N/A
Recovery	N/A

51.8 tmnxOspfFailureDisabled

Table 891: tmnxOspfFailureDisabled properties

Property name	Value
Application name	OSPF
Event ID	2038
Event name	tmnxOspfFailureDisabled
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.38
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: OSPF disabled. Reason: *$tmnx OspfFailureReasonCode$*
Cause	N/A
Effect	N/A
Recovery	N/A

51.9 tmnxOspfLsdbApproachingOverflow

Table 892: tmnxOspfLsdbApproachingOverflow properties

Property name	Value
Application name	OSPF
Event ID	2015
Event name	tmnxOspfLsdbApproachingOverflow

Property name	Value
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.15
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Number of external LSAs has exceed 90% of the configured limit (*$tmnxOspfExtLsdbLimit$*)
Cause	The number of external LSAs in the router's link-state database has exceeded ninety percent of the configured limit.
Effect	N/A
Recovery	N/A

51.10 tmnxOspfLsdbOverflow

Table 893: tmnxOspfLsdbOverflow properties

Property name	Value
Application name	OSPF
Event ID	2014
Event name	tmnxOspfLsdbOverflow
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.14
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Number of external LSAs has exceeded the configured limit (*$tmnxOspfExtLsdbLimit$*)
Cause	The number of external LSAs in the router's link-state database has exceeded the configured limit.
Effect	N/A
Recovery	N/A

51.11 tmnxOspfNgIfAuthFailure

Table 894: tmnxOspfNgIfAuthFailure properties

Property name	Value
Application name	OSPF

Property name	Value
Event ID	2044
Event name	tmnxOspfNgIfAuthFailure
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.44
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Packet failed *$tmnxOspfConfig ErrorType$* authentication on interface *$ospfIfIpAddress$* from *$tmnx OspfPacketSrcAddress$* in *$tmnxOspfPacketType$*
Cause	A packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
Effect	N/A
Recovery	N/A

51.12 tmnxOspfNgIfConfigError

Table 895: tmnxOspfNgIfConfigError properties

Property name	Value
Application name	OSPF
Event ID	2043
Event name	tmnxOspfNgIfConfigError
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.43
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Conflicting configuration *$tmnx OspfConfigErrorType$* on interface *$ospfIfIpAddress$* from *$tmnxOspf PacketSrcAddress$* in *$tmnxOspfPacketType$*
Cause	A packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event 'optionMismatch' should cause a trap only if it prevents an adjacency from forming.
Effect	N/A
Recovery	N/A

51.13 tmnxOspfNgIfRxBadPacket

Table 896: tmnxOspfNgIfRxBadPacket properties

Property name	Value
Application name	OSPF
Event ID	2045
Event name	tmnxOspfNgIfRxBadPacket
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.45
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Bad packet, *$tmnxOspfBadPacketErrType$*, received on interface *$ospfIfIpAddress$* from *$tmnxOspfPacketSrcAddress$* in *$tmnxOspfPacketType$*
Cause	An OSPF packet has been received on a non-virtual interface that cannot be parsed.
Effect	N/A
Recovery	N/A

51.14 tmnxOspfNgIfStateChange

Table 897: tmnxOspfNgIfStateChange properties

Property name	Value
Application name	OSPF
Event ID	2047
Event name	tmnxOspfNgIfStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.47
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Interface *$tmnxOspfIfIpName$* state changed to *$tmnxOspfNgIfState$* (event *$tmnxOspfIfEvent$*)
Cause	There has been a change in the state of a non-virtual OSPF interface. This event is generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup).

Property name	Value
Effect	N/A
Recovery	N/A

51.15 tmnxOspfNgIfTxRetransmit

Table 898: tmnxOspfNgIfTxRetransmit properties

Property name	Value
Application name	OSPF
Event ID	2046
Event name	tmnxOspfNgIfTxRetransmit
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.46
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Retransmit to neighbor *$ospfNbr RtrId$* on interface *$ospfIfIpAddress$*
Cause	An OSPF packet has been retransmitted on a non-virtual interface. All packets that may be retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.
Effect	N/A
Recovery	N/A

51.16 tmnxOspfNgLdpSyncExit

Table 899: tmnxOspfNgLdpSyncExit properties

Property name	Value
Application name	OSPF
Event ID	2052
Event name	tmnxOspfNgLdpSyncExit
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.52
Default severity	warning

Property name	Value
Message format string	IGP-LDP synchronization has stopped for interface *$vRtrIfIndex$* because *$strReason$*.
Cause	N/A
Effect	N/A
Recovery	N/A

51.17 tmnxOspfNgLdpSyncTimerStarted

Table 900: tmnxOspfNgLdpSyncTimerStarted properties

Property name	Value
Application name	OSPF
Event ID	2051
Event name	tmnxOspfNgLdpSyncTimerStarted
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.51
Default severity	warning
Message format string	IGP-LDP synchronization timer has started for interface *$vRtrIfIndex$*.
Cause	The OSPF interface LDP synchronization timer state has started. The timer was started from the time the LDP session to the neighbor became up over the interface. This is to allow for the label FEC bindings to be exchanged.
Effect	N/A
Recovery	N/A

51.18 tmnxOspfNgLinkMaxAgeLsa

Table 901: tmnxOspfNgLinkMaxAgeLsa properties

Property name	Value
Application name	OSPF
Event ID	2050
Event name	tmnxOspfNgLinkMaxAgeLsa

Property name	Value
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.50
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Max aged LSA *$ospfLsdbLsid$* type *$ospfLsdbType$* ifIndex *$ospfLinkIfIdx$* ifInstId *$ospfLinkIfInstId$* advertising router *$ospfLsdbRtrId$*
Cause	One of the LSAs in the router's link-state database has reached its maximum age limit.
Effect	N/A
Recovery	N/A

51.19 tmnxOspfNgLinkOriginateLsa

Table 902: tmnxOspfNgLinkOriginateLsa properties

Property name	Value
Application name	OSPF
Event ID	2049
Event name	tmnxOspfNgLinkOriginateLsa
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.49
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Originated LSA *$ospfLsdbLsid$* type *$ospfLsdbType$* ifIndex *$ospfLinkIfIdx$* ifInstId *$ospfLinkIfInstId$* advertising router *$ospfLsdbRtrId$*
Cause	A new LSA has been originated by this router. This event is not generated for simple refreshes of LSAs (which happens every 30 minutes), but instead is only generated when an LSA is (re)originated due to a topology change. Additionally, this event does not include LSAs that are being flushed because they have reached their maximum age limit.
Effect	N/A
Recovery	N/A

51.20 tmnxOspfNgNbrRestartHlprStsChg

Table 903: tmnxOspfNgNbrRestartHlprStsChg properties

Property name	Value
Application name	OSPF
Event ID	2048
Event name	tmnxOspfNgNbrRestartHlprStsChg
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.48
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Helper status for neighbor *$ospfNbrIpAddr$* router *$ospfNbrRtrId$* changed to *$tmnxOspfNgNbrRestartHelperStatus$* (Helper Age *$tmnxOspfNgNbrRestartHelperAge$* Exit Reason *$tmnxOspfNgNbrRestartHelperExitRc$*)
Cause	There has been a change in the graceful restart helper state for the neighbor. This event is generated when the neighbor restart helper status transitions for a neighbor.
Effect	N/A
Recovery	N/A

51.21 tmnxOspfNgNbrStateChange

Table 904: tmnxOspfNgNbrStateChange properties

Property name	Value
Application name	OSPF
Event ID	2042
Event name	tmnxOspfNgNbrStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.42
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Neighbor *$ospfNbrRtrId$* on *$ospfNbrIpAddr$* router state changed to *$tmnxOspfNgNbrState$* (event *$ospfNbrEvent$*)
Cause	There has been a change in the state of a non-virtual OSPF neighbor. This event is generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal

Property name	Value
	state (e.g., 2-Way or Full). When a neighbor transitions from or to Full on non-broadcast multi-access and broadcast networks, the event is generated by the designated router. A designated router transitioning to Down is indicated by the value of ospfNgIfStateChange.
Effect	N/A
Recovery	N/A

51.22 tmnxOspfNssaTranslatorStatusChg

Table 905: tmnxOspfNssaTranslatorStatusChg properties

Property name	Value
Application name	OSPF
Event ID	2017
Event name	tmnxOspfNssaTranslatorStatusChg
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.17
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: NSSA translator state in area *$ospfAreaId$* changed to *$tmnxOspfAreaNssaTranslatorState$*
Cause	There has been a change in the router's ability to translate OSPF type-7 LSAs into OSPF type-5 LSAs. This event is generated when the Translator Status transitions from or to any defined status on a per area basis.
Effect	N/A
Recovery	N/A

51.23 tmnxOspfOverloadEntered

Table 906: tmnxOspfOverloadEntered properties

Property name	Value
Application name	OSPF
Event ID	2023

Property name	Value
Event name	tmnxOspfOverloadEntered
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.23
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Overload entered (event *$tmnx OspfLastOverloadEnterCode$*) *$tmnxOspfNotifyDescription$*
Cause	OSPF entered the overload state. vRtrOspfLastOverloadEnterCode holds the condition which caused OSPF to get into overload.
Effect	N/A
Recovery	N/A

51.24 tmnxOspfOverloadExited

Table 907: tmnxOspfOverloadExited properties

Property name	Value
Application name	OSPF
Event ID	2024
Event name	tmnxOspfOverloadExited
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.24
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Overload exited (event *$tmnx OspfLastOverloadExitCode$*)
Cause	OSPF entered the overload state. vRtrOspfLastOverloadExitCode holds the condition which caused OSPF to get out of overload.
Effect	N/A
Recovery	N/A

51.25 tmnxOspfOverloadWarning

Table 908: tmnxOspfOverloadWarning properties

Property name	Value
Application name	OSPF
Event ID	2055
Event name	tmnxOspfOverloadWarning
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.55
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Reached 80 percent overload limit (event *$tmnxOspfLastOverloadEnterCode$*) *$tmnxOspfNotify Description$*
Cause	A tmnxOspfOverloadWarning trap is sent out when OSPF reaches 80 percent of overload limit. tmnxOspfLastOverloadEnterCode holds the condition which caused OSPF to approach this limit.
Effect	N/A
Recovery	N/A

51.26 tmnxOspfRejectedAdjacencySid

Table 909: tmnxOspfRejectedAdjacencySid properties

Property name	Value
Application name	OSPF
Event ID	2056
Event name	tmnxOspfRejectedAdjacencySid
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.56
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Rejected adjacency SID *$tmnx OspfNotifyDescription$*
Cause	The tmnxOspfRejectedAdjacencySid notification is sent when we do not establish an adjacency SID or adjacency PGID due to a lack of resources. This should be an edge-triggered notification. We should not send a second notification about adjacency SID allocation failure for

Property name	Value
	the same adjacency. We should not send a second notification about adjacency PGID allocation failure for the same adjacency.
Effect	No effect.
Recovery	Whenever an ADJ-SID is released, the released ADJ-SID can be reused by any other adjacency which is waiting to receive an ADJ-SID. Whenever a PGID is released, the released PGID can be reused by any other adjacency which is waiting to receive a PGID.

51.27 tmnxOspfRestartStatusChange

Table 910: tmnxOspfRestartStatusChange properties

Property name	Value
Application name	OSPF
Event ID	2018
Event name	tmnxOspfRestartStatusChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.18
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Restart status changed to *$tmnxOspfRestartStatus$* (Restart Interval *$tmnxOspfRestartInterval$* Exit Reason *$tmnxOspfRestartExitRc$*)
Cause	There has been a change in the graceful restart state for the router. This event is generated when the router restart status changes.
Effect	N/A
Recovery	N/A

51.28 tmnxOspfRoutesExpLmtDropped

Table 911: tmnxOspfRoutesExpLmtDropped properties

Property name	Value
Application name	OSPF
Event ID	2041

Property name	Value
Event name	tmnxOspfRoutesExpLmtDropped
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.41
Default severity	warning
Message format string	The number of redistributed routes into OSPF has dropped below the export limit *$tmnxOspfExportLimit$*
Cause	Number of exported routes is dropped below the configured export limit.
Effect	N/A
Recovery	N/A

51.29 tmnxOspfShamIfAuthFailure

Table 912: tmnxOspfShamIfAuthFailure properties

Property name	Value
Application name	OSPF
Event ID	2034
Event name	tmnxOspfShamIfAuthFailure
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.34
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Packet failed *$tmnxOspfConfig ErrorType$* authentication from sham-link neighbor *$tmnxOspfSham IfRemoteNbrAddress$* in *$tmnxOspfPacketType$*
Cause	N/A
Effect	N/A
Recovery	N/A

51.30 tmnxOspfShamIfConfigError

Table 913: tmnxOspfShamIfConfigError properties

Property name	Value
Application name	OSPF
Event ID	2033
Event name	tmnxOspfShamIfConfigError
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.33
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Conflicting configuration *$tmnxOspfConfigErrorType$* from sham-link neighbor *$tmnxOspfShamIfRemoteNbrAddress$* in *$tmnxOspfPacketType$*
Cause	N/A
Effect	N/A
Recovery	N/A

51.31 tmnxOspfShamIfRxBadPacket

Table 914: tmnxOspfShamIfRxBadPacket properties

Property name	Value
Application name	OSPF
Event ID	2035
Event name	tmnxOspfShamIfRxBadPacket
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.35
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Bad packet, *$tmnxOspfBadPacketErrType$*, received from sham-link neighbor *$tmnxOspfShamIfRemoteNbrAddress$* in *$tmnxOspfPacketType$*
Cause	N/A
Effect	N/A
Recovery	N/A

51.32 tmnxOspfShamIfStateChange

Table 915: tmnxOspfShamIfStateChange properties

Property name	Value
Application name	OSPF
Event ID	2031
Event name	tmnxOspfShamIfStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.31
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*:State of sham-link interface *$tmnxOspfShamIfIndex$* with neighbor *$tmnxOspfShamIfRemoteNbrAddress$* changed to *$tmnxOspfShamIfState$*
Cause	N/A
Effect	N/A
Recovery	N/A

51.33 tmnxOspfShamIfTxRetransmit

Table 916: tmnxOspfShamIfTxRetransmit properties

Property name	Value
Application name	OSPF
Event ID	2036
Event name	tmnxOspfShamIfTxRetransmit
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.36
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Retransmit to sham-link interface *$tmnxOspfShamNbrIfIndex$*
Cause	N/A
Effect	N/A
Recovery	N/A

51.34 tmnxOspfShamNbrRestartHlprStsChg

Table 917: tmnxOspfShamNbrRestartHlprStsChg properties

Property name	Value
Application name	OSPF
Event ID	2037
Event name	tmnxOspfShamNbrRestartHlprStsChg
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.37
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Helper status for sham-link neighbor *$tmnxOspfShamNbrRtrId$* changed to *$tmnxOspfShamNbr RestartHelperStatus$* (Helper Age *$tmnxOspfShamNbrRestartHelper Age$* Exit Reason *$tmnxOspfShamNbrRestartHelperExitRc$*)
Cause	N/A
Effect	N/A
Recovery	N/A

51.35 tmnxOspfShamNbrStateChange

Table 918: tmnxOspfShamNbrStateChange properties

Property name	Value
Application name	OSPF
Event ID	2032
Event name	tmnxOspfShamNbrStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.32
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: State of sham-link neighbor *$tmnxOspfShamNbrRtrId$* changed to *$tmnxOspfShamNbrState$*
Cause	N/A
Effect	N/A

Property name	Value
Recovery	N/A

51.36 tmnxOspfSpfRunsRestarted

Table 919: tmnxOspfSpfRunsRestarted properties

Property name	Value
Application name	OSPF
Event ID	2022
Event name	tmnxOspfSpfRunsRestarted
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.22
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: SPF runs resumed - memory resources available
Cause	There are sufficient memory resources on the system to start running the SPF to completion.
Effect	OSPF will resume running the SPFs as required.
Recovery	N/A

51.37 tmnxOspfSpfRunsStopped

Table 920: tmnxOspfSpfRunsStopped properties

Property name	Value
Application name	OSPF
Event ID	2021
Event name	tmnxOspfSpfRunsStopped
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.21
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: SPF runs stopped - insufficient memory resources

Property name	Value
Cause	There are insufficient memory resources on the system to run the SPF to completion.
Effect	OSPF stops running SPFs until enough memory resources become available.
Recovery	Free some memory resources.

51.38 tmnxOspfSrgbBadLabelRange

Table 921: tmnxOspfSrgbBadLabelRange properties

Property name	Value
Application name	OSPF
Event ID	2058
Event name	tmnxOspfSrgbBadLabelRange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.58
Default severity	warning
Message format string	Bad SRGB label range for advertising router: *$tmnxOspfNotifSrgbAdvRtrID$*, startLabel:*$tmnxOspfNotifSrgbRangeStartLbl$*, maxIdx: *$tmnxOspfNotifSrgbRangeMaxIdx$*, area:*$tmnxOspfNotifSrgbAreaId$*
Cause	The tmnxOspfSrgbBadLabelRange notification is sent when OSPF receives a bad SRGB label range from a router (e.g. overlapping with another label range.
Effect	The configured Segment Routing tunnels will be wrong.
Recovery	Change the label range to recover.

51.39 tmnxOspfSrSidError

Table 922: tmnxOspfSrSidError properties

Property name	Value
Application name	OSPF
Event ID	2053
Event name	tmnxOspfSrSidError

Property name	Value
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.53
Default severity	minor
Message format string	Received SID label already in use for other prefix, reason: *$tmnxOspfNotifyDescription$*
Cause	This notification is generated when OSPF receives an IOM or CPM failure (system exhausted ILM, NHLFE, duplicate SID) while resolving and programming a received prefix SID.
Effect	The Segment Routing tunnel corresponding to this SID will not be programmed.
Recovery	In case of system exhaustion, the IGP instance goes into overload. The operator must manually clear the IGP overload condition after freeing resources. IGP will attempt to program at the next SPF all tunnels which previously failed the programming operation.

51.40 tmnxOspfSrSidNotInLabelRange

Table 923: tmnxOspfSrSidNotInLabelRange properties

Property name	Value
Application name	OSPF
Event ID	2054
Event name	tmnxOspfSrSidNotInLabelRange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.54
Default severity	minor
Message format string	Receivd SID not in range *$tmnxOspfNotifPfxSidRangeStartLbl$*(+*$tmnxOspfNotifPfxSidRangeMaxIdx$*)of NH-router *$tmnxOspfNotifPfxNhAdvRtr$*
Cause	This notification is generated when OSPF receives a SID which is not within the label range of the nhop router.
Effect	The Segment Routing tunnel corresponding to this SID will not be programmed.
Recovery	Increase the label range or change the SID index to be within the current label range.

51.41 tmnxOspfVirtIfAuthFailure

Table 924: tmnxOspfVirtIfAuthFailure properties

Property name	Value
Application name	OSPF
Event ID	2007
Event name	tmnxOspfVirtIfAuthFailure
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.7
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Packet failed *$tmnxOspfConfigErrorType$* authentication from virtual neighbor *$ospfVirtIfNeighbor$* area *$ospfVirtIfAreaId$* in *$tmnxOspfPacketType$*
Cause	A packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
Effect	N/A
Recovery	N/A

51.42 tmnxOspfVirtIfConfigError

Table 925: tmnxOspfVirtIfConfigError properties

Property name	Value
Application name	OSPF
Event ID	2005
Event name	tmnxOspfVirtIfConfigError
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.5
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Conflicting configuration *$tmnxOspfConfigErrorType$* from virtual neighbor *$ospfVirtIfNeighbor$* area *$ospfVirtIfAreaId$* in *$tmnxOspfPacketType$*
Cause	A packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration

Property name	Value
	parameters. Note that the event optionMismatch should generate an event only if it prevents an adjacency from forming.
Effect	N/A
Recovery	N/A

51.43 tmnxOspfVirtIfRxBadPacket

Table 926: tmnxOspfVirtIfRxBadPacket properties

Property name	Value
Application name	OSPF
Event ID	2009
Event name	tmnxOspfVirtIfRxBadPacket
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.9
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Bad packet, *$tmnxOspfBadPacketErrType$* received from virtual neighbor *$ospfVirtIfNeighbor$* area *$ospfVirtIfAreaId$* in *$tmnxOspfPacketType$*
Cause	An OSPF packet that cannot be parsed has been received on a virtual interface.
Effect	N/A
Recovery	N/A

51.44 tmnxOspfVirtIfStateChange

Table 927: tmnxOspfVirtIfStateChange properties

Property name	Value
Application name	OSPF
Event ID	2001
Event name	tmnxOspfVirtIfStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.1

Property name	Value
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Virtual interface *$ospfVirtIfNeighbor$* in transit-area *$ospfVirtIfAreaId$* state changed to *$tmnxOspfVirtIfState$* (event *$ospfVirtIfEvent$*)
Cause	There has been a change in the state of an OSPF virtual interface. This event is generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).
Effect	N/A
Recovery	N/A

51.45 tmnxOspfVirtIfTxRetransmit

Table 928: tmnxOspfVirtIfTxRetransmit properties

Property name	Value
Application name	OSPF
Event ID	2011
Event name	tmnxOspfVirtIfTxRetransmit
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.11
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Retransmit to virtual interface *$ospfVirtIfNeighbor$* in transit-area *$ospfVirtIfAreaId$*
Cause	An OSPF packet has been retransmitted on a virtual interface. All packets that may be retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.
Effect	N/A
Recovery	N/A

51.46 tmnxOspfVirtNbrRestartHlprStsChg

Table 929: tmnxOspfVirtNbrRestartHlprStsChg properties

Property name	Value
Application name	OSPF
Event ID	2020
Event name	tmnxOspfVirtNbrRestartHlprStsChg
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.20
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Helper status for Virtual neighbor *$ospfVirtNbrRtrId$* in transit-area *$ospfVirtNbrArea$* changed to *$tmnxOspfVirtNbrRestartHelperStatus$* (Helper Age *$tmnxOspfVirtNbrRestartHelperAge$* Exit Reason *$tmnxOspfVirtNbrRestartHelperExitRc$*)
Cause	There has been a change in the graceful restart helper state for the virtual neighbor. This event is generated when the virtual neighbor restart helper status transitions for a virtual neighbor.
Effect	N/A
Recovery	N/A

51.47 tmnxOspfVirtNbrStateChange

Table 930: tmnxOspfVirtNbrStateChange properties

Property name	Value
Application name	OSPF
Event ID	2003
Event name	tmnxOspfVirtNbrStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.3
Default severity	warning
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Virtual neighbor *$ospfVirtNbrRtrId$* in transit-area *$ospfVirtNbrArea$* state changed to *$tmnxOspfVirtNbrState$* (event *$ospfVirtNbrEvent$*)
Cause	There has been a change in the state of an OSPF virtual neighbor. This event is generated when the neighbor state regresses (e.g., goes from

Property name	Value
	Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).
Effect	N/A
Recovery	N/A

52 PCAP

52.1 tmnxPcapBufferFull

Table 931: tmnxPcapBufferFull properties

Property name	Value
Application name	PCAP
Event ID	2002
Event name	tmnxPcapBufferFull
SNMP notification prefix and OID	TIMETRA-PCAP-MIB.tmnxPcapNofitications.2
Default severity	minor
Message format string	Session *$tmnxPcapSessionName$*'s allocated buffer is full, with size *$tmnxPcapSessionBufferSize$*. Total number of packets dropped by this session is *$tmnxPcapSessionDroppedPackets$* pacekts.
Cause	A tmnxPcapBufferFull notification is generated when the PCAP session allocated buffer is full, indicating a higher traffic rate.
Effect	May result in dropping packets, if not recoverable.
Recovery	The software will eventually recover when all the buffer contents are uploaded to the capture file. No action required.

52.2 tmnxPcapBufferReadWriteFailure

Table 932: tmnxPcapBufferReadWriteFailure properties

Property name	Value
Application name	PCAP
Event ID	2003
Event name	tmnxPcapBufferReadWriteFailure
SNMP notification prefix and OID	TIMETRA-PCAP-MIB.tmnxPcapNofitications.3
Default severity	major

Property name	Value
Message format string	Session *$tmnxPcapSessionName$* has encountered a buffer read/write failure. Total read failures: *$tmnxPcapSessionBufReadFailures$*, total write failures: *$tmnxPcapSessionBufWriteFailures$*.
Cause	A tmnxPcapBufferReadWriteFailure notification is generated when a read or write operation to the PCAP session buffer fails.
Effect	Will result in dropping packets.
Recovery	The software will potentially recover. No action may be required. However, if the problem persists stop the packet capture, delete and re-configure a new PCAP session.

52.3 tmnxPcapFileError

Table 933: tmnxPcapFileError properties

Property name	Value
Application name	PCAP
Event ID	2001
Event name	tmnxPcapFileError
SNMP notification prefix and OID	TIMETRA-PCAP-MIB.tmnxPcapNofitications.1
Default severity	minor
Message format string	Session *$tmnxPcapSessionName$* has encountered a capture file operation related error. Session is in *$tmnxPcapSessionState$* state.
Cause	A tmnxPcapFileError notification is generated when a PCAP session encounters a capture file operation related error.
Effect	The packet capture may not be uploaded to the PCAP file anymore, or the capture may be inaccurate.
Recovery	Check the file-url, and user-permissions specified. Stop the packet capture, remove and re-configure a new file-url, and start the capture again.

52.4 tmnxPcapSoftwareFailure

Table 934: tmnxPcapSoftwareFailure properties

Property name	Value
Application name	PCAP
Event ID	2004
Event name	tmnxPcapSoftwareFailure
SNMP notification prefix and OID	TIMETRA-PCAP-MIB.tmnxPcapNofitications.4
Default severity	major
Message format string	Session *$tmnxPcapSessionName$* has encountered a software failure. Session is in *$tmnxPcapSessionState$* state.
Cause	A tmnxPcapSoftwareFailure notification is generated when a software failure occurs, affecting the ability of the PCAP session to perform its task.
Effect	Will result in dropping packets.
Recovery	Stop the packet capture, delete and re-configure a new PCAP session.

53 PIM

53.1 aluVRtrPimNgSGLimitExceeded

Table 935: aluVRtrPimNgSGLimitExceeded properties

Property name	Value
Application name	PIM
Event ID	3001
Event name	aluVRtrPimNgSGLimitExceeded
SNMP notification prefix and OID	ALU-VRTR-MIB.aluVRtrNotifications.4
Default severity	warning
Message format string	TODO
Cause	The aluVRtrPimNgSGLimitExceeded notification is generated when the number of (S,G) groups transitions between exceeding and falling below a system limit defined based on the 7705 platform.
Effect	N/A
Recovery	N/A

53.2 aluVRtrPimNgUnsupportedStarG

Table 936: aluVRtrPimNgUnsupportedStarG properties

Property name	Value
Application name	PIM
Event ID	3000
Event name	aluVRtrPimNgUnsupportedStarG
SNMP notification prefix and OID	ALU-VRTR-MIB.aluVRtrNotifications.3
Default severity	warning
Message format string	TODO

Property name	Value
Cause	The aluVRtrPimNgUnsupportedStarG notification is generated when the router receives a register message, a (*,G) assert message, a (*,G) Join Prune message or a (*,G) IGMP local membership message.
Effect	N/A
Recovery	N/A

53.3 vRtrPimNgBSRStateChange

Table 937: vRtrPimNgBSRStateChange properties

Property name	Value
Application name	PIM
Event ID	2006
Event name	vRtrPimNgBSRStateChange
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.6
Default severity	minor
Message format string	BSR state changed to *$vRtrPimNgAFGenBSRState$*
Cause	There was a change in the BSR state on the router. The managed object vRtrPimNgGenBSRState indicates the current BSR state.
Effect	N/A
Recovery	N/A

53.4 vRtrPimNgDataMtReused

Table 938: vRtrPimNgDataMtReused properties

Property name	Value
Application name	PIM
Event ID	2012
Event name	vRtrPimNgDataMtReused
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.12

Property name	Value
Default severity	warning
Message format string	The selective provider tunnel with index *$vRtrPimNgDataMtIfIndex$* configured for source address *$vRtrPimNgDataMtMdSourceAddress$* and group address *$vRtrPimNgDataMtMdGroupAddress$* has now *$vRtrPimNgDataMtNumVpnSGs$* or more C(S,G)s after being reused by C(S,G) (*$DataMtCGrpSrcSourceAddr$*,*$DataMtCGrpSrcGroupAddr$*)
Cause	A selective provider tunnel was reused, i.e. a C (S,G) was mapped to a selective provider tunnel that is already in use by another C (S,G).
Effect	N/A
Recovery	N/A

53.5 vRtrPimNgGrpInSSMRange

Table 939: vRtrPimNgGrpInSSMRange properties

Property name	Value
Application name	PIM
Event ID	2005
Event name	vRtrPimNgGrpInSSMRange
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.5
Default severity	warning
Message format string	Received *$vRtrPimNgNotifyMsgType$* message on interface *$vRtrIfIndex$* for group *$vRtrPimNgNotifyGroupAddr$* which is in the SSM group range.
Cause	The router received a register message, a (*,G) assert message, a (*,G) Join Prune message or a IGMP local membership message for the group defined in the SSM address range.
Effect	N/A
Recovery	N/A

53.6 vRtrPimNgHelloDropped

Table 940: vRtrPimNgHelloDropped properties

Property name	Value
Application name	PIM
Event ID	2007
Event name	vRtrPimNgHelloDropped
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.7
Default severity	warning
Message format string	Hello from neighbor *$vRtrPimNgIfNeighborAddress$* on interface *$vRtrIfIndex$* dropped because the multicast sender attribute on this interface is set to 'always'
Cause	A hello was dropped because the multicast sender attribute on the interface is set to 'always'.
Effect	N/A
Recovery	N/A

53.7 vRtrPimNgIfNeighborLoss

Table 941: vRtrPimNgIfNeighborLoss properties

Property name	Value
Application name	PIM
Event ID	2001
Event name	vRtrPimNgIfNeighborLoss
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.1
Default severity	minor
Message format string	Lost adjacency with neighbor *$vRtrPimNgIfNeighborAddress$* on interface *$vRtrIfIndex$*
Cause	The PIM adjacency with a neighbor was lost.
Effect	N/A
Recovery	N/A

53.8 vRtrPimNgIfNeighborUp

Table 942: vRtrPimNgIfNeighborUp properties

Property name	Value
Application name	PIM
Event ID	2002
Event name	vRtrPimNgIfNeighborUp
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.2
Default severity	minor
Message format string	Adjacency with neighbor *$vRtrPimNgIfNeighborAddress$* on interface *$vRtrIfIndex$* came up
Cause	A PIM adjacency with a new neighbor was established.
Effect	N/A
Recovery	N/A

53.9 vRtrPimNgInvalidIPmsiTunnel

Table 943: vRtrPimNgInvalidIPmsiTunnel properties

Property name	Value
Application name	PIM
Event ID	2014
Event name	vRtrPimNgInvalidIPmsiTunnel
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.14
Default severity	warning
Message format string	Received intra-as a/d route with invalid i-pmsi tunnel group address *$vRtrPimNgWrongMdtDefGrpAddr$* from *$vRtrPimNgNotifySourceIp$*, expected *$vRtrPimNgAFGenMdtDefGrpAddress$*
Cause	The vRtrPimNgInvalidIPmsiTunnel event is generated when an invalid default core group address specified by vRtrPimNgWrong MdtDefGrpAddr of the Multicast Distribution Tree(MDT) is received in PIM message from vRtrPimNgNotifySourceIp, instead of the expected addresss specified by vRtrPimNgAFGenMdtDefGrpAddress.

Property name	Value
	It is considered to be a misconfiguration and the message will be dropped. This trap is intended to help network operators recognize the misconfiguration and adjust their configurations accordingly. This event is also generated when the tunnel type specified by vRtrPimNgWrong PmsiType is received in PIM message from vRtrPimNgNotifySourceIp which is different from the configured tunnel type.
Effect	The PMSI received in the PIM message from vRtrPimNgNotifySourceIp is not processed by PIM.
Recovery	Operator needs to look and adjust the configuration of vRtrPim NgNotifySourceIp in the VPRN specified by vRtrPimNgWrongVprnId. The objects vRtrPimNgWrongPmsiP2mpId, vRtrPimNgWrongPmsi TunnelId and vRtrPimNgWrongPmsiExtTunlAddr in the event vRtrPim NgInvalidIPmsiTunnel are valid only when vRtrPimNgWrongPmsiType is 'rsvp (2)'. The objects vRtrPimNgWrongMdtDefGrpAddrType and v RtrPimNgWrongMdtDefGrpAddr in the event vRtrPimNgInvalidIPmsi Tunnel are valid only when vRtrPimNgWrongPmsiType is either 'pim Ssm (0)' or 'pimSm (1)'. The objects vRtrPimNgWrongPmsiLdpLspId, v RtrPimNgWrongPmsiSenderAdrTyp and vRtrPimNgWrongPmsiSender Addr in the event vRtrPimNgInvalidIPmsiTunnel are valid only when v RtrPimNgWrongPmsiType is 'ldp (3)'.

53.10 vRtrPimNgInvalidJoinPrune

Table 944: vRtrPimNgInvalidJoinPrune properties

Property name	Value
Application name	PIM
Event ID	2003
Event name	vRtrPimNgInvalidJoinPrune
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.3
Default severity	warning
Message format string	Received invalid Join Prune message from *$vRtrPimNgNotifySource Ip$* with RP address *$vRtrPimNgNotifyWrongRPAddr$* for group *$vRtr PimNgNotifyGroupAddr$*. Correct RP address for the group is *$vRtr PimNgNotifyRPAddr$*(0.0.0.0 if unknown)
Cause	An invalid Join Prune message was received. A Join Prune message is deemed invalid when there is an RP address disagreement between the router and the PIM Join Prune message.
Effect	N/A

Property name	Value
Recovery	N/A

53.11 vRtrPimNgInvalidRegister

Table 945: vRtrPimNgInvalidRegister properties

Property name	Value
Application name	PIM
Event ID	2004
Event name	vRtrPimNgInvalidRegister
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.4
Default severity	warning
Message format string	Received invalid Register message from *$vRtrPimNgNotifySourceIp$* with RP address *$vRtrPimNgNotifyWrongRPAddr$* for group *$vRtrPim NgNotifyGroupAddr$*. Correct RP address for the group is *$vRtrPim NgNotifyRPAddr$*(0.0.0.0 if unknown)
Cause	An invalid PIM Register message was received. A Register message is deemed invalid when there is an RP address disagreement between the router and the PIM Register message.
Effect	N/A
Recovery	N/A

53.12 vRtrPimNgMaxGraftRetry

Table 946: vRtrPimNgMaxGraftRetry properties

Property name	Value
Application name	PIM
Event ID	2015
Event name	vRtrPimNgMaxGraftRetry
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.15
Default severity	minor

Property name	Value
Message format string	Exceeded *$vRtrPimNgNumGraftRetriesExcd$* retries for source address *$vRtrPimNgNotifySourceAddr$*, group address *$vRtrPim NgNotifyGroupAddr$* and will stop trying.
Cause	The vRtrPimNgMaxGraftRetry is generated when the number of graft retries has exceeded 10.
Effect	We will stop retrying sending of graft messages and remain in ack-pending state.
Recovery	The recovery is caused by a subsequent graft ack or data which will move the state to forwarding.

53.13 vRtrPimNgMaxGrpsLimitExceeded

Table 947: vRtrPimNgMaxGrpsLimitExceeded properties

Property name	Value
Application name	PIM
Event ID	2011
Event name	vRtrPimNgMaxGrpsLimitExceeded
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.11
Default severity	warning
Message format string	The number of groups configured on the interface *$ifName$* has exceeded the maximum limit of *$vRtrPimNgIfMaxGroups$*
Cause	An attempt was made to configure a group when the number of groups configured on the interface has exeeeded the maximum limit.
Effect	N/A
Recovery	N/A

53.14 vRtrPimNgMcacPlcyDropped

Table 948: vRtrPimNgMcacPlcyDropped properties

Property name	Value
Application name	PIM

Property name	Value
Event ID	2013
Event name	vRtrPimNgMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.13
Default severity	warning
Message format string	Group *$vRtrPimNgNotifyGroupAddr$* is dropped because of multicast CAC policy *$vRtrPimNgIfMcacPolicyName$* on interface *$ifName$* PIM instance *$vRtrID$*
Cause	A PIM group was dropped on a given interface because of applying a multicast CAC policy.
Effect	N/A
Recovery	N/A

53.15 vRtrPimNgMDTLimitExceeded

Table 949: vRtrPimNgMDTLimitExceeded properties

Property name	Value
Application name	PIM
Event ID	2010
Event name	vRtrPimNgMDTLimitExceeded
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.10
Default severity	warning
Message format string	The selective provider tunnel configuration failed for PIM instance *$vRtrID$*, maximum selective provider tunnel limit of *$vRtrPimNgGenMaxMdts$* exceeded
Cause	The configuration exceeded the maximum number of selective provider tunnels supported on the system.
Effect	N/A
Recovery	N/A

53.16 vRtrPimNgReplicationLmtExceeded

Table 950: vRtrPimNgReplicationLmtExceeded properties

Property name	Value
Application name	PIM
Event ID	2009
Event name	vRtrPimNgReplicationLmtExceeded
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.9
Default severity	warning
Message format string	Maximum number of replications reached for (S,G), (*$vRtrPimNgNotifySourceIp$*, *$vRtrPimNgNotifyGroupAddr$*) on IOM *$tmnxCardHwIndex$*, failed to program OIF record
Cause	An IOM failed to program an OIF for an (S,G) record because the replication limit for that (S,G) on that IOM has been reached. The replication limit per (S,G) entry on an IOM is currently 127.
Effect	N/A
Recovery	N/A

53.17 vRtrPimNgSGLimitExceeded

Table 951: vRtrPimNgSGLimitExceeded properties

Property name	Value
Application name	PIM
Event ID	2008
Event name	vRtrPimNgSGLimitExceeded
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.8
Default severity	warning
Message format string	Maximum number of multicast (S,G) records reached on IOM *$tmnxCardHwIndex$*, failed to program OIF record
Cause	A (S,G) record failed to be programmed to an IOM because the supported (S,G) limit was exceeded. This limit is currently at 16000 (S,G) entries.
Effect	N/A

Property name	Value
Recovery	N/A

54 PIM_SNOOPING

54.1 tmnxPimSnpgIfNeighborLoss

Table 952: tmnxPimSnpgIfNeighborLoss properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2001
Event name	tmnxPimSnpgIfNeighborLoss
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.1
Default severity	minor
Message format string	Lost neighbor *$tmnxPimSnpgIfNbrAddress$* on *$ifName$*
Cause	The PIM adjacency with a neighbor was lost.
Effect	N/A
Recovery	N/A

54.2 tmnxPimSnpgIfNeighborUp

Table 953: tmnxPimSnpgIfNeighborUp properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2002
Event name	tmnxPimSnpgIfNeighborUp
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.2
Default severity	minor
Message format string	Snooped new neighbor *$tmnxPimSnpgIfNbrAddress$* on *$ifName$*
Cause	The PIM adjacency with a new neighbor was established.

Property name	Value
Effect	N/A
Recovery	N/A

54.3 tmnxPimSnpgSGLimitExceeded

Table 954: tmnxPimSnpgSGLimitExceeded properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2003
Event name	tmnxPimSnpgSGLimitExceeded
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.3
Default severity	warning
Message format string	Maximum number of multicast (S,G) records reached on IOM *$tmnxCardHwIndex$*, failed to program OIF record
Cause	A (S,G) record failed to be programmed to an IOM because the supported (S,G) limit was exceeded. This limit is currently at 16000 (S,G) entries.
Effect	N/A
Recovery	N/A

54.4 tmnxPimSnpgSnoopModeChanged

Table 955: tmnxPimSnpgSnoopModeChanged properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2004
Event name	tmnxPimSnpgSnoopModeChanged
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.4
Default severity	warning

Property name	Value
Message format string	PIM-Snooping Operational Mode changed to *$tmnxPimSnpgGenOperState$*. Configured mode is *$tmnxPimSnpgGenMode$*
Cause	A snooping mode was changed from proxy to snoop or vice versa.
Effect	N/A
Recovery	N/A

55 PORT

55.1 SFPStatusBlocked

Table 956: SFPStatusBlocked properties

Property name	Value
Application name	PORT
Event ID	2060
Event name	SFPStatusBlocked
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Message format string	SFF blocked by culprit
Cause	The tmnxEqPortSFPStatusFailure notification is generated when the tmnxPortSFPStatus of an SFF results in a value other than 'not-equipped (0)', or 'operational (1)'. tmnxEqPortSFPStatusFailure obsoleted tmnxEqPortSFPCorrupted for revision 6.0 on Nokia SROS series systems.
Effect	The SFF device is not operational and the associated port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

55.2 SFPStatusCulprit

Table 957: SFPStatusCulprit properties

Property name	Value
Application name	PORT
Event ID	2059
Event name	SFPStatusCulprit
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36

Property name	Value
Default severity	minor
Message format string	SFF is culprit
Cause	The tmnxEqPortSFPStatusFailure notification is generated when the tmnxPortSFPStatus of an SFF results in a value other than 'not-equipped (0)', or 'operational (1)'. tmnxEqPortSFPStatusFailure obsoleted tmnxEqPortSFPCorrupted for revision 6.0 on Nokia SROS series systems.
Effect	The SFF device is not operational and the associated port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

55.3 SFPStatusDDMCorrupt

Table 958: SFPStatusDDMCorrupt properties

Property name	Value
Application name	PORT
Event ID	2031
Event name	SFPStatusDDMCorrupt
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Message format string	SFP/XFP DDM Checksums do not match
Cause	The tmnxEqPortSFPStatusFailure notification is generated when the tmnxPortSFPStatus of an SFF results in a value other than 'not-equipped (0)', or 'operational (1)'. tmnxEqPortSFPStatusFailure obsoleted tmnxEqPortSFPCorrupted for revision 6.0 on Nokia SROS series systems.
Effect	The SFF device is not operational and the associated port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

55.4 SFPStatusFailure

Table 959: SFPStatusFailure properties

Property name	Value
Application name	PORT
Event ID	2008
Event name	SFPStatusFailure
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Message format string	SFF Checksums do not match
Cause	The tmnxEqPortSFPStatusFailure notification is generated when the tmnxPortSFPStatus of an SFF results in a value other than 'not-equipped (0)', or 'operational (1)'. tmnxEqPortSFPStatusFailure obsoleted tmnxEqPortSFPCorrupted for revision 6.0 on Nokia SROS series systems.
Effect	The SFF device is not operational and the associated port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

55.5 SFPStatusOperational

Table 960: SFPStatusOperational properties

Property name	Value
Application name	PORT
Event ID	2061
Event name	SFPStatusOperational
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Message format string	SFF operational
Cause	The event is generated when the SFF does not undergo a removal or insertion but it recovers from an error state. This can happen when an SFF device with tmnxPortSFPStatus 'culprit (6)' is removed, and

Property name	Value
	the state of the other affected SFF devices with tmnxPortSFPStatus 'blocked (7)' clear back to tmnxPortSFPStatus 'operational (1)'.
Effect	The SFF device is operational.
Recovery	N/A

55.6 SFPStatusReadError

Table 961: SFPStatusReadError properties

Property name	Value
Application name	PORT
Event ID	2032
Event name	SFPStatusReadError
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Message format string	SFP/XFP Read failure
Cause	The tmnxEqPortSFPStatusFailure notification is generated when the tmnxPortSFPStatus of an SFF results in a value other than 'not-equipped (0)', or 'operational (1)'. tmnxEqPortSFPStatusFailure obsoleted tmnxEqPortSFPCorrupted for revision 6.0 on Nokia SROS series systems.
Effect	The SFF device is not operational and the associated port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

55.7 SFPStatusUnsupported

Table 962: SFPStatusUnsupported properties

Property name	Value
Application name	PORT
Event ID	2033

Property name	Value
Event name	SFPStatusUnsupported
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Message format string	SFP/XFP unsupported type
Cause	The tmnxEqPortSFPStatusFailure notification is generated when the tmnxPortSFPStatus of an SFF results in a value other than 'not-equipped (0)', or 'operational (1)'. tmnxEqPortSFPStatusFailure obsoleted tmnxEqPortSFPCorrupted for revision 6.0 on Nokia SROS series systems.
Effect	The SFF device is not operational and the associated port can not be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

55.8 tdcmAlarms

Table 963: tdcmAlarms properties

Property name	Value
Application name	PORT
Event ID	2043
Event name	tdcmAlarms
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.45
Default severity	minor
Message format string	Optical Tdcm Alarms Set *$tmnxOpticalPortTdcmAlarmState$*
Cause	The tmnxEqPortOpticalTdcmAlarm notification indicates that an Optical Tdcm interface has experienced either a raising or clearing of an alarm as indicated by the value of tmnxOpticalPortTdcmAlarmState.
Effect	N/A
Recovery	N/A

55.9 tmnxBundleMemberMlfrLoopback

Table 964: tmnxBundleMemberMlfrLoopback properties

Property name	Value
Application name	PORT
Event ID	2035
Event name	tmnxBundleMemberMlfrLoopback
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.39
Default severity	minor
Message format string	Mlfr Bundle Member *$tmnxPortPortID$* Loopback *$tmnxBundleMemberMlfrDownReason$*
Cause	Generated when a Multilink Frame-Relay Bundle Member enters or leaves the 'loopback (3)' state.
Effect	N/A
Recovery	N/A

55.10 tmnxDS1E1LoopbackStarted

Table 965: tmnxDS1E1LoopbackStarted properties

Property name	Value
Application name	PORT
Event ID	2019
Event name	tmnxDS1E1LoopbackStarted
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.24
Default severity	minor
Message format string	DS1/E1 '*$tmnxDS1Loopback$*' Loopback Started
Cause	The tmnxDS1E1LoopbackStarted notification is generated when a loopback is provisioned on a DS1/E1 port.
Effect	N/A
Recovery	N/A

55.11 tmnxDS1E1LoopbackStopped

Table 966: tmnxDS1E1LoopbackStopped properties

Property name	Value
Application name	PORT
Event ID	2020
Event name	tmnxDS1E1LoopbackStopped
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.25
Default severity	minor
Message format string	DS1/E1 '*$tmnxDS1Loopback$*' Loopback Stopped
Cause	The tmnxDS1E1LoopbackStopped notification is generated when a loopback is removed on a DS1/E1 port. The value of tmnxSonet Loopback specifies the type of loopback that was configured and has now been removed.
Effect	N/A
Recovery	N/A

55.12 tmnxDS3E3LoopbackStarted

Table 967: tmnxDS3E3LoopbackStarted properties

Property name	Value
Application name	PORT
Event ID	2021
Event name	tmnxDS3E3LoopbackStarted
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.26
Default severity	minor
Message format string	DS3/E3 '*$tmnxDS3ChannelLoopback$*' Loopback Started
Cause	The tmnxDS3E3LoopbackStarted notification is generated when a loopback is provisioned on a DS3/E3 port.
Effect	N/A

Property name	Value
Recovery	N/A

55.13 tmnxDS3E3LoopbackStopped

Table 968: tmnxDS3E3LoopbackStopped properties

Property name	Value
Application name	PORT
Event ID	2022
Event name	tmnxDS3E3LoopbackStopped
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.27
Default severity	minor
Message format string	DS3/E3 '*$tmnxDS3ChannelLoopback$*' Loopback Stopped
Cause	The tmnxDS3E3LoopbackStopped notification is generated when a loopback is removed on a DS3/E3 port. The value of tmnxDS3Channel Loopback specifies the type of loopback that was configured and has now been removed.
Effect	N/A
Recovery	N/A

55.14 tmnxDSXClockSyncStateChange

Table 969: tmnxDSXClockSyncStateChange properties

Property name	Value
Application name	PORT
Event ID	2034
Event name	tmnxDSXClockSyncStateChange
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.37
Default severity	minor
Message format string	Clock Sync State (*$tmnxDSXClockSyncStateObject$*)

Property name	Value
Cause	Generated when the tmnxDS3ChannelClockSyncState changes for a DS3 or DS1 channel with adaptive or differentical clock source.
Effect	N/A
Recovery	N/A

55.15 tmnxEqCohOptPortAlarm

Table 970: tmnxEqCohOptPortAlarm properties

Property name	Value
Application name	PORT
Event ID	2056
Event name	tmnxEqCohOptPortAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.56
Default severity	minor
Message format string	Coherent Optical Alarms Active: *$tmnxCohOptPortAlarmState$*
Cause	The tmnxEqCohOptAlarmState notification indicates that a coherent optical port has experienced either a raising or a clearing of an alarm as indicated by the value of tmnxCohOptPortAlarmState. Further details can be obtained from the value of tmnxCohOptPortDefect Points.
Effect	N/A
Recovery	N/A

55.16 tmnxEqDigitalDiagMonitorClear

Table 971: tmnxEqDigitalDiagMonitorClear properties

Property name	Value
Application name	PORT
Event ID	2041
Event name	tmnxEqDigitalDiagMonitorClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.43
Default severity	minor
Message format string	XFP/SFP DDM (*$tmnxDDMFailedObject$*) cleared
Cause	Generated when an SFP/XFP that supports Digital Diagnostic Monitoring (DDM) clears a failed state.
Effect	N/A
Recovery	N/A

55.17 tmnxEqDigitalDiagMonitorFailure

Table 972: tmnxEqDigitalDiagMonitorFailure properties

Property name	Value
Application name	PORT
Event ID	2030
Event name	tmnxEqDigitalDiagMonitorFailure
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.35
Default severity	minor
Message format string	SFF DDM *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailedObject$*) raised
Cause	Generated when an SFF that supports Digital Diagnostic Monitoring (DDM) enters a failed state.
Effect	N/A
Recovery	N/A

55.18 tmnxEqPortBndlBadEndPtDiscr

Table 973: tmnxEqPortBndlBadEndPtDiscr properties

Property name	Value
Application name	PORT

Property name	Value
Event ID	2012
Event name	tmnxEqPortBndlBadEndPtDiscr
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.21
Default severity	minor
Message format string	Port *$tmnxPortPortId$* detected inconsistent peer endpoint discriminator for the bundle
Cause	Generated when the port detected mismatched peer endpoint discriminator for the bundle.
Effect	N/A
Recovery	N/A

55.19 tmnxEqPortBndlRedDiffExceeded

Table 974: tmnxEqPortBndlRedDiffExceeded properties

Property name	Value
Application name	PORT
Event ID	2011
Event name	tmnxEqPortBndlRedDiffExceeded
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.20
Default severity	major
Message format string	Port *$tmnxPortNotifyPortId$* exceeded red differential delay of *$tmnx BundleRedDiffDelay$*
Cause	Generated when the differential delay of a port in the bundle exceeds the configured value in tmnxBundleRedDiffDelay.
Effect	N/A
Recovery	N/A

55.20 tmnxEqPortBndlYellowDiffExceeded

Table 975: tmnxEqPortBndlYellowDiffExceeded properties

Property name	Value
Application name	PORT
Event ID	2010
Event name	tmnxEqPortBndlYellowDiffExceeded
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.19
Default severity	minor
Message format string	Port *$tmnxPortNotifyPortId$* exceeded yellow differential delay of *$tmnxBundleYellowDiffDelay$*
Cause	Generated when the differential delay of a port in the bundle exceeds the configured value in tmnxBundleYellowDiffDelay.
Effect	N/A
Recovery	N/A

55.21 tmnxEqPortDS1Alarm

Table 976: tmnxEqPortDS1Alarm properties

Property name	Value
Application name	PORT
Event ID	2015
Event name	tmnxEqPortDS1Alarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.17
Default severity	minor
Message format string	Alarm *$tmnxPortNotifyDS1AlarmReason$* Set
Cause	Generated when a DS1 interface alarm condition is detected. It is generated only when the type of alarm being raised is enabled in tmnxDS1ReportAlarm.
Effect	N/A
Recovery	N/A

55.22 tmnxEqPortDS1AlarmClear

Table 977: tmnxEqPortDS1AlarmClear properties

Property name	Value
Application name	PORT
Event ID	2016
Event name	tmnxEqPortDS1AlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.18
Default severity	minor
Message format string	Alarm *$tmnxPortNotifyDS1AlarmReason$* Cleared
Cause	Generated when a DS1 interface alarm condition is cleared. It is generated only when the type of alarm being cleared is enabled in tmnxDS1ReportAlarm.
Effect	N/A
Recovery	N/A

55.23 tmnxEqPortDS3Alarm

Table 978: tmnxEqPortDS3Alarm properties

Property name	Value
Application name	PORT
Event ID	2013
Event name	tmnxEqPortDS3Alarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.15
Default severity	minor
Message format string	Alarm *$tmnxPortNotifyDS3AlarmReason$* Set
Cause	Generated when a DS3 interface alarm condition is detected. It is generated only when the type of alarm being raised is enabled in tmnxDS3ChannelReportAlarm.
Effect	N/A

Property name	Value
Recovery	N/A

55.24 tmnxEqPortDS3AlarmClear

Table 979: tmnxEqPortDS3AlarmClear properties

Property name	Value
Application name	PORT
Event ID	2014
Event name	tmnxEqPortDS3AlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.16
Default severity	minor
Message format string	Alarm *$tmnxPortNotifyDS3AlarmReason$* Cleared
Cause	Generated when a DS3 interface alarm condition is cleared. It is generated only when the type of alarm being cleared is enabled in tmnxDS3ChannelReportAlarm.
Effect	N/A
Recovery	N/A

55.25 tmnxEqPortDuplexCfgNotCompatible

Table 980: tmnxEqPortDuplexCfgNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2028
Event name	tmnxEqPortDuplexCfgNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.33
Default severity	major
Message format string	Provisioned duplex *$tmnxPortEtherDuplex$* not compatible with MDA type *$tmnxMdaNotifyTyp$*

Property name	Value
Cause	Generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible with the currently provisioned MDA, but the currently configured duplex on an MDA port is not compatible with the inserted MDA.
Effect	N/A
Recovery	N/A

55.26 tmnxEqPortError

Table 981: tmnxEqPortError properties

Property name	Value
Application name	PORT
Event ID	2009
Event name	tmnxEqPortError
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.14
Default severity	minor
Message format string	Physical port *$tmnxPortNotifyError$*
Cause	Generated when an error listed in tmnxPortNotifyError is detected on the port.
Effect	N/A
Recovery	N/A

55.27 tmnxEqPortEtherAlarm

Table 982: tmnxEqPortEtherAlarm properties

Property name	Value
Application name	PORT
Event ID	2017
Event name	tmnxEqPortEtherAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.22

Property name	Value
Default severity	minor
Message format string	Alarm *$tmnxPortNotifyEtherAlarmReason$* Set
Cause	tmnxEqPortEtherAlarm is generated when a ethernet port alarm condition is detected. It is generated only when the type of alarm being raised is enabled in tmnxPortEtherReportAlarm.
Effect	N/A
Recovery	N/A

55.28 tmnxEqPortEtherAlarmClear

Table 983: tmnxEqPortEtherAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2018
Event name	tmnxEqPortEtherAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.23
Default severity	minor
Message format string	Alarm *$tmnxPortNotifyEtherAlarmReason$* Cleared
Cause	tmnxEqPortEtherAlarmClear is generated when a ethernet port alarm condition is cleared. It is generated only when the type of alarm being cleared is enabled in tmnxPortEtherReportAlarm.
Effect	N/A
Recovery	N/A

55.29 tmnxEqPortEtherCrcAlarm

Table 984: tmnxEqPortEtherCrcAlarm properties

Property name	Value
Application name	PORT
Event ID	2052

Property name	Value
Event name	tmnxEqPortEtherCrcAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.52
Default severity	minor
Message format string	CRC errors in excess of the configured *$tmnxPortNotifyEtherCrcAlarm Value$* threshold *$tmnxPortNotifyEtherCrcMultiplier$*10e- *$tmnxPort NotifyEtherCrcThreshold$* Set
Cause	tmnxEqPortEtherCrcAlarm is generated when an Ethernet port CRC alarm condition is detected. It is generated only when the type of alarm being raised is enabled on the port.
Effect	On a signal failure (SF) fault, the port is taken out of service until the CRC alarm condition is cleared.
Recovery	tmnxEqPortEtherCrcAlarm is cleared by taking the port out of service (eg. shutdown, card/mda reset, physical link loss), or changing/ disabling the associated threshold/multiplier values. Signal Degradation is self clearing and will clear once the error rate drops below 1/10th of the configured rate.

55.30 tmnxEqPortEtherCrcAlarmClear

Table 985: tmnxEqPortEtherCrcAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2053
Event name	tmnxEqPortEtherCrcAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.53
Default severity	minor
Message format string	CRC errors in excess of the configured *$tmnxPortNotifyEtherCrcAlarm Value$* threshold *$tmnxPortNotifyEtherCrcMultiplier$*10e- *$tmnxPort NotifyEtherCrcThreshold$* Cleared
Cause	tmnxEqPortEtherCrcAlarmClear is generated when an Ethernet port CRC alarm condition is cleared or disabled.
Effect	N/A
Recovery	N/A

55.31 tmnxEqPortEtherInternalAlarm

Table 986: tmnxEqPortEtherInternalAlarm properties

Property name	Value
Application name	PORT
Event ID	2054
Event name	tmnxEqPortEtherInternalAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.54
Default severity	minor
Message format string	Excess internal MAC TX errors detected Set
Cause	tmnxEqPortEtherInternalAlarm is generated when an Ethernet port experiences excessive internal MAC tx errors. It is generated only when tmnxPortEtherDownOnInternalError is enabled on the port.
Effect	A port experiencing excessive internal MAC tx errors will take the port out of service while the alarm condition is in affect.
Recovery	tmnxEqPortEtherInternalAlarm is cleared by taking the port out of service (eg. shutdown, card/mda reset, physical link loss), or setting tmnxPortEtherDownOnInternalError to the value 'false'.

55.32 tmnxEqPortEtherInternalAlarmClr

Table 987: tmnxEqPortEtherInternalAlarmClr properties

Property name	Value
Application name	PORT
Event ID	2055
Event name	tmnxEqPortEtherInternalAlarmClr
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.55
Default severity	minor
Message format string	Excess internal MAC TX errors detected Cleared
Cause	tmnxEqPortEtherInternalAlarmClr is generated when an Ethernet port no longer experiences excessive internal MAC tx errors.

Property name	Value
Effect	N/A
Recovery	N/A

55.33 tmnxEqPortEtherLoopCleared

Table 988: tmnxEqPortEtherLoopCleared properties

Property name	Value
Application name	PORT
Event ID	2026
Event name	tmnxEqPortEtherLoopCleared
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.31
Default severity	minor
Message format string	Ethernet loop cleared on *$tmnxPortNotifyPortId$*
Cause	The tmnxEqPortEtherLoopCleared notification is generated when down-when-looped detects an Ethernet port has stopped receiving PDUs that it transmitted and tmnxPortEtherDownWhenLoopedEnabled is set to 'true'. Setting tmnxPortEtherDownWhenLoopedEnabled to 'false' will also cause this notification to be generated if tmnxEqPort EtherLoopDetected had previously been raised.
Effect	N/A
Recovery	N/A

55.34 tmnxEqPortEtherLoopDetected

Table 989: tmnxEqPortEtherLoopDetected properties

Property name	Value
Application name	PORT
Event ID	2025
Event name	tmnxEqPortEtherLoopDetected
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.30

Property name	Value
Default severity	minor
Message format string	Ethernet loop detected on *$tmnxPortNotifyPortId$*
Cause	The tmnxEqPortEtherLoopDetected notification is genereated when down-when-looped detects an Ethernet port is receiving PDUs that it transmitted and tmnxPortEtherDownWhenLoopedEnabled is set to 'true'.
Effect	N/A
Recovery	N/A

55.35 tmnxEqPortEtherSymMonAlarm

Table 990: tmnxEqPortEtherSymMonAlarm properties

Property name	Value
Application name	PORT
Event ID	2057
Event name	tmnxEqPortEtherSymMonAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.57
Default severity	minor
Message format string	Symbol errors in excess of the configured *$tmnxPortNotifyEtherSymAlarmValue$* threshold *$tmnxPortNotifyEtherSymMultiplier$**10e-*$tmnxPortNotifyEtherSymThreshold$* Set
Cause	tmnxEqPortEtherSymMonAlarm is generated when an Ethernet port Symbol alarm condition is detected. It is generated only when the type of alarm being raised is enabled on the port.
Effect	On a signal failure (SF) fault, the port is taken out of service until the Symbol alarm condition is cleared.
Recovery	tmnxEqPortEtherSymMonAlarm is cleared by taking the port out of service (eg. shutdown, card/mda reset, physical link loss), or changing/disabling the associated threshold/multiplier values. Signal Degradation is self clearing and will clear once the error rate drops below 1/10th of the configured rate.

55.36 tmnxEqPortEtherSymMonAlarmClear

Table 991: tmnxEqPortEtherSymMonAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2058
Event name	tmnxEqPortEtherSymMonAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.58
Default severity	minor
Message format string	Symbol errors in excess of the configured *$tmnxPortNotifyEtherSymAlarmValue$* threshold *$tmnxPortNotifyEtherSymMultiplier$**10e-*$tmnxPortNotifyEtherSymThreshold$* Cleared
Cause	tmnxEqPortEtherSymMonAlarmClear is generated when an Ethernet port Symbol alarm condition is cleared or disabled.
Effect	N/A
Recovery	N/A

55.37 tmnxEqPortIngressRateCfgNotCompatible

Table 992: tmnxEqPortIngressRateCfgNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2029
Event name	tmnxEqPortIngressRateCfgNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.34
Default severity	major
Message format string	Ingress rate provisioning not supported on MDA type *$tmnxMdaNotifyType$*
Cause	Generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible with the currently provisioned MDA, but the currently configured ingress rate on an MDA port is not compatible with the inserted MDA.
Effect	N/A

Property name	Value
Recovery	N/A

55.38 tmnxEqPortOpticalAmpAlarm

Table 993: tmnxEqPortOpticalAmpAlarm properties

Property name	Value
Application name	PORT
Event ID	2042
Event name	tmnxEqPortOpticalAmpAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.44
Default severity	minor
Message format string	Optical Amplifier Alarms Set *$tmnxOpticalPortTdcmAlarmState$*
Cause	The tmnxEqPortOpticalAmpAlarm notification indicates that an Optical Amplifier interface has experienced either a raising or clearing of an alarm as indicated by the value of tmnxOpticalPortAmpAlarmState.
Effect	N/A
Recovery	N/A

55.39 tmnxEqPortSFPInserted

Table 994: tmnxEqPortSFPInserted properties

Property name	Value
Application name	PORT
Event ID	2005
Event name	tmnxEqPortSFPInserted
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.8
Default severity	minor
Message format string	SFF Inserted
Cause	Generated when a SFP is inserted in the port.

Property name	Value
Effect	N/A
Recovery	N/A

55.40 tmnxEqPortSFPRemoved

Table 995: tmnxEqPortSFPRemoved properties

Property name	Value
Application name	PORT
Event ID	2006
Event name	tmnxEqPortSFPRemoved
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.9
Default severity	minor
Message format string	SFF Removed
Cause	Generated when a SFP is removed from the port.
Effect	N/A
Recovery	N/A

55.41 tmnxEqPortSonetAlarm

Table 996: tmnxEqPortSonetAlarm properties

Property name	Value
Application name	PORT
Event ID	2001
Event name	tmnxEqPortSonetAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.4
Default severity	minor
Message format string	Alarm *$tmnxPortNotifySonetAlarmReason$* Set

Property name	Value
Cause	Generated when a SONET/SDH port alarm condition is detected. It is generated only when the type of alarm being raised is enabled in tmnx SonetReportAlarm.
Effect	N/A
Recovery	N/A

55.42 tmnxEqPortSonetAlarmClear

Table 997: tmnxEqPortSonetAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2002
Event name	tmnxEqPortSonetAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.5
Default severity	minor
Message format string	Alarm *$tmnxPortNotifySonetAlarmReason$* Cleared
Cause	Generated when a SONET/SDH port alarm condition is cleared. It is generated only when the type of alarm being cleared is enabled in tmnx SonetReportAlarm.
Effect	N/A
Recovery	N/A

55.43 tmnxEqPortSonetPathAlarm

Table 998: tmnxEqPortSonetPathAlarm properties

Property name	Value
Application name	PORT
Event ID	2003
Event name	tmnxEqPortSonetPathAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.6

Property name	Value
Default severity	minor
Message format string	Alarm *$tmnxPortNotifySonetPathAlarmReason$* Set
Cause	Generated when a SONET/SDH path alarm condition is detected. It is generated only when the type of alarm being raised is enabled in tmnx SonetPathReportAlarm.
Effect	N/A
Recovery	N/A

55.44 tmnxEqPortSonetPathAlarmClear

Table 999: tmnxEqPortSonetPathAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2004
Event name	tmnxEqPortSonetPathAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.7
Default severity	minor
Message format string	Alarm *$tmnxPortNotifySonetPathAlarmReason$* Cleared
Cause	Generated when a SONET/SDH path alarm condition is cleared. It is generated only when the type of alarm being cleared is enabled in tmnx SonetPathReportAlarm.
Effect	N/A
Recovery	N/A

55.45 tmnxEqPortSpeedCfgNotCompatible

Table 1000: tmnxEqPortSpeedCfgNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2027

Property name	Value
Event name	tmnxEqPortSpeedCfgNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.32
Default severity	major
Message format string	Provisioned speed *$tmnxPortEtherSpeed$* not compatible with MDA type *$tmnxMdaNotifyType$*
Cause	Generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible with the currently provisioned MDA, but the currently configured speed on an MDA port is not compatible with the inserted MDA.
Effect	N/A
Recovery	N/A

55.46 tmnxEqPortWaveTrackerAlarm

Table 1001: tmnxEqPortWaveTrackerAlarm properties

Property name	Value
Application name	PORT
Event ID	2038
Event name	tmnxEqPortWaveTrackerAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.40
Default severity	minor
Message format string	WaveTracker Alarms Set *$tmnxPortNotifyWTAlarmReason$*
Cause	The tmnxEqPortWaveTrackerAlarm notification indicates that a Wave Tracker interface has experienced either a raising or clearing of an alarm as indicated by the value of tmnxPortNotifyWTAlarmReason.
Effect	N/A
Recovery	N/A

55.47 tmnxEqSonetClockSrcNotCompatible

Table 1002: tmnxEqSonetClockSrcNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2046
Event name	tmnxEqSonetClockSrcNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.46
Default severity	major
Message format string	Configured SONET/SDH clock source *$tmnxSonetClockSource$* not compatible with MDA type *$tmnxMdaNotifyType$*
Cause	Notification tmnxEqSonetClockSrcNotCompatible is generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible with the currently provisioned MDA, but the currently configured SONET/SDH clock source on an MDA port is not compatible with the inserted MDA.
Effect	Though services can still be created, the MDA will fail to operate as configured and will be in a failed state.
Recovery	Change the configuration to reflect the capabilities of the MDA port, or switch out the MDA for one that is compatible.

55.48 tmnxEqSonetFramingNotCompatible

Table 1003: tmnxEqSonetFramingNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2048
Event name	tmnxEqSonetFramingNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.48
Default severity	major
Message format string	Configured SONET/SDH framing *$tmnxSonetFraming$* not compatible with MDA type *$tmnxMdaNotifyType$*
Cause	Notification tmnxEqSonetFramingNotCompatible is generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible

Property name	Value
	with the currently provisioned MDA, but the currently configured SONET/SDH framing on an MDA port is not compatible with the inserted MDA.
Effect	Though services can still be created, the MDA will fail to operate as configured and will be in a failed state.
Recovery	Change the configuration to reflect the capabilities of the MDA port, or switch out the MDA for one that is compatible.

55.49 tmnxEqSonetSfThreshNotCompatible

Table 1004: tmnxEqSonetSfThreshNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2047
Event name	tmnxEqSonetSfThreshNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.47
Default severity	major
Message format string	Configured SONET/SDH SF threshold 10e- *$tmnxSonetBer SfThreshold$* not compatible with MDA type *$tmnxMdaNotifyType$*
Cause	Notification tmnxEqSonetSfThreshNotCompatible is generated when a supported MDA is inserted into a slot of an IOM, the MDA is compatible with the currently provisioned MDA, but the currently configured SONET/SDH Signal Fail (SF) threshold on an MDA port is not compatible with the inserted MDA.
Effect	Though services can still be created, the MDA will fail to operate as configured and will be in a failed state.
Recovery	Change the configuration to reflect the capabilities of the MDA port, or switch out the MDA for one that is compatible.

55.50 tmnxOesPortError

Table 1005: tmnxOesPortError properties

Property name	Value
Application name	PORT
Event ID	3001
Event name	tmnxOesPortError
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.15
Default severity	critical
Message format string	OES Port Error: *$tmnxOesPortNotifyError$*
Cause	The tmnxOesPortError notification is generated when an error condition listed in tmnxOesPortNotifyError is detected on the OES port.
Effect	The OES port is experiencing errors that could be service affecting.
Recovery	tmnxOesPortError is cleared by taking the port out of service, eg. shutdown, or try a soft reset, hard reset, then replacement of the card if the error condition persists.

55.51 tmnxOesPortErrorClear

Table 1006: tmnxOesPortErrorClear properties

Property name	Value
Application name	PORT
Event ID	3002
Event name	tmnxOesPortErrorClear
SNMP notification prefix and OID	TIMETRA-OES-HARDWARE-MIB.tmnxOesHwNotifications.16
Default severity	critical
Message format string	All OES Port Errors Cleared
Cause	The tmnxOesPortErrorClear notification is generated when all error conditions on the OES port are cleared.
Effect	The OES port error conditions are cleared.
Recovery	No recovery required.

55.52 tmnxOtuIfAlarmNotification

Table 1007: tmnxOtuIfAlarmNotification properties

Property name	Value
Application name	PORT
Event ID	2037
Event name	tmnxOtuIfAlarmNotification
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxOtuNotifications.1
Default severity	minor
Message format string	OTU Alarms Set *$tmnxOtuIfAlarmState$*
Cause	The tmnxOtuIfAlarmNotification notification indicates that an OTU interface has experienced either a raising or clearing of an alarm in the Forward Error Correction (FEC), Section Monitoring (SM), Path Monitoring (PM) or Payload Monitoring (PSI) fields of the OTU frame.
Effect	N/A
Recovery	N/A

55.53 tmnxPortUnsupportedFunction

Table 1008: tmnxPortUnsupportedFunction properties

Property name	Value
Application name	PORT
Event ID	2036
Event name	tmnxPortUnsupportedFunction
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.38
Default severity	minor
Message format string	A functionality is required from port *$tmnxPortNotifyPortId$* that it cannot support - *$tmnxPortNotifyDescription$*
Cause	Generated when a functionality is required from this port that it cannot support. The object tmnxPortNotifyDescription explains what function is affected.

Property name	Value
Effect	N/A
Recovery	N/A

55.54 tmnxResvCbsPoolThreshAmber

Table 1009: tmnxResvCbsPoolThreshAmber properties

Property name	Value
Application name	PORT
Event ID	2050
Event name	tmnxResvCbsPoolThreshAmber
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.50
Default severity	minor
Message format string	Amber Alarm: CBS over Amber threshold: ObjType= *$tmnxObjType $* Owner=*$tmnxObjPortId$* Type=*$tmnxObjAppType$* Pool= *$tmnx ObjAppPool$* NamedPoolPolicy=*$tmnxObjNamedPoolPolicy$* Resv Size= *$tmnxObjAppResvSize$* SumOfQ ResvSize=*$tmnxObjApp SumOfQResvSize$* Old ResvCBS= *$tmnxObjAppResvCbsOld$* New ResvCBS=*$tmnxObjAppResvCbsNew$* Old ResvSize= *$tmnxObjApp ResvSizeOld$*
Cause	The notification tmnxResvCbsPoolThreshAmber is generated when a reserved-CBS of an object (MDA or port) has crossed threshold value specified by tmnxObjectAppAmbrAlrmThresh.
Effect	This is warning event but the traffic is not yet affected.
Recovery	The value of tmnxObjectAppResvCbs or TIMETRA-QOS-MIB::tQ1NamedPoolReservedCbs may need to be adjusted.

55.55 tmnxResvCbsPoolThreshGreen

Table 1010: tmnxResvCbsPoolThreshGreen properties

Property name	Value
Application name	PORT
Event ID	2049

Property name	Value
Event name	tmnxResvCbsPoolThreshGreen
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.49
Default severity	minor
Message format string	Green Alarm: CBS within threshold: ObjType= *$tmnxObjType$* Owner= *$tmnxObjPortId$* Type=*$tmnxObjAppType$* Pool= *$tmnxObjAppPool$* NamedPoolPolicy=*$tmnxObjNamedPoolPolicy$* ResvSize= *$tmnxObjAppResvSize$* SumOfQ ResvSize=*$tmnxObjAppSumOfQResvSize$* Old ResvCBS= *$tmnxObjAppResvCbsOld$* New ResvCBS=*$tmnxObjAppResvCbsNew$* Old ResvSize= *$tmnxObjAppResvSizeOld$*
Cause	Notification tmnxResvCbsPoolThreshGreen is generated when a reserved- CBS of an object (MDA or port) returns to within defined thresholds.
Effect	Reserved CBS of the object has returned to within normal parameters.
Recovery	None required.

55.56 tmnxResvCbsPoolThreshRed

Table 1011: tmnxResvCbsPoolThreshRed properties

Property name	Value
Application name	PORT
Event ID	2051
Event name	tmnxResvCbsPoolThreshRed
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.51
Default severity	major
Message format string	Red Alarm: CBS over Red threshold: ObjType= *$tmnxObjType$* Owner=*$tmnxObjPortId$* Type=*$tmnxObjAppType$* Pool= *$tmnxObjAppPool$* NamedPoolPolicy=*$tmnxObjNamedPoolPolicy$* Resv Size= *$tmnxObjAppResvSize$* SumOfQ ResvSize=*$tmnxObjAppSumOfQResvSize$* Old ResvCBS= *$tmnxObjAppResvCbsOld$* New ResvCBS=*$tmnxObjAppResvCbsNew$* Old ResvSize= *$tmnxObjAppResvSizeOld$*
Cause	The notification tmnxResvCbsPoolThreshAmber is generated when a reserved-CBS of an object (MDA or port) has crossed the threshold value specified by tmnxObjectAppRedAlrmThresh.

Property name	Value
Effect	This is a critical event and the traffic may be affected.
Recovery	The value of tmnxObjectAppResvCbs or TIMETRA-QOS-MIB::tQ1NamedPoolReservedCbs may need to be adjusted.

55.57 tmnxSonetSDHLoopbackStarted

Table 1012: tmnxSonetSDHLoopbackStarted properties

Property name	Value
Application name	PORT
Event ID	2023
Event name	tmnxSonetSDHLoopbackStarted
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.28
Default severity	minor
Message format string	Sonet/SDH '*$tmnxSonetLoopback$*' Loopback Started
Cause	The tmnxSonetSDHLoopbackStarted notification is generated when a loopback is provisioned on a Sonet-SDH port.
Effect	N/A
Recovery	N/A

55.58 tmnxSonetSDHLoopbackStopped

Table 1013: tmnxSonetSDHLoopbackStopped properties

Property name	Value
Application name	PORT
Event ID	2024
Event name	tmnxSonetSDHLoopbackStopped
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.29
Default severity	minor
Message format string	Sonet/SDH '*$tmnxSonetLoopback$*' Loopback Stopped

Property name	Value
Cause	The tmnxSonetSDHLoopbackStopped notification is generated when a loopback test is removed on a Sonet-SDH port. The value of tmnxDS1Loopback specifies the type of loopback that was configured and has now been removed.
Effect	N/A
Recovery	N/A

55.59 tPortAccEgrQGrpHostMatchFailure

Table 1014: tPortAccEgrQGrpHostMatchFailure properties

Property name	Value
Application name	PORT
Event ID	2039
Event name	tPortAccEgrQGrpHostMatchFailure
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.41
Default severity	minor
Message format string	Could not find a specific port egress queue-group for host with inter-dest-id ' *$tmnxHostMatchNotifyIntDestId$*', org-string '*$tmnxHostMatchNotifyOrgString$*' and sub-id ' *$tmnxHostMatchNotifySubIdent$*' on port *$tmnxPortNotifyPortId$*. The default 'policer-output-queues' queue-group will be used.
Cause	The tPortAccEgrQGrpHostMatchFailure notification indicates that a host match lookup failed to resolve a specific port egress queue-group. In such case the default policer-output-queue is used.
Effect	N/A
Recovery	N/A

55.60 tPortEgrVPortHostMatchFailure

Table 1015: tPortEgrVPortHostMatchFailure properties

Property name	Value
Application name	PORT

Property name	Value
Event ID	2040
Event name	tPortEgrVPortHostMatchFailure
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.42
Default severity	minor
Message format string	Could not find a specific port egress virtual port for host with inter-dest-id ' *$tmnxHostMatchNotifyIntDestId$*', org-string '*$tmnxHostMatch NotifyOrgString$*' and sub-id ' *$tmnxHostMatchNotifySubIdent$*' on port *$tmnxPortNotifyPortId$*
Cause	The tPortEgrVPortHostMatchFailure notification indicates that a host match lookup failed to resolve a specific port egress virtual port.
Effect	N/A
Recovery	N/A

56 PPP

56.1 ipcpPeerOnDifferentSubnet

Table 1016: ipcpPeerOnDifferentSubnet properties

Property name	Value
Application name	PPP
Event ID	2011
Event name	ipcpPeerOnDifferentSubnet
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* remote IP address *$remoteIpAddr$* is not on the local subnet *$localSubnet$*
Cause	The peer is not on the local subnet.
Effect	N/A
Recovery	No recovery is necessary.

56.2 ipcpPeerRejectedOurIp

Table 1017: ipcpPeerRejectedOurIp properties

Property name	Value
Application name	PPP
Event ID	2010
Event name	ipcpPeerRejectedOurIp
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* local IP address *$localIpAddr$* negotiation rejected by remote

Property name	Value
Cause	The peer rejected our IP address configuration request.
Effect	N/A
Recovery	No recovery is necessary.

56.3 ipcpPeerSuggestedDifferentIp

Table 1018: ipcpPeerSuggestedDifferentIp properties

Property name	Value
Application name	PPP
Event ID	2009
Event name	ipcpPeerSuggestedDifferentIp
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* local IP address *$localIpAddr$* different from IP address *$remoteIpAddr$* suggested by remote
Cause	The peer suggested a different IP via a 'confnak' message.
Effect	N/A
Recovery	No recovery is necessary.

56.4 ipcpRemoteIpUnknown

Table 1019: ipcpRemoteIpUnknown properties

Property name	Value
Application name	PPP
Event ID	2007
Event name	ipcpRemoteIpUnknown
SNMP notification prefix and OID	N/A
Default severity	warning

Property name	Value
Message format string	Port *$subject$* remote IP address is unknown
Cause	The remote IP address is unknown.
Effect	N/A
Recovery	No recovery is necessary.

56.5 ipcpSameLocalAndRemoteIp

Table 1020: ipcpSameLocalAndRemoteIp properties

Property name	Value
Application name	PPP
Event ID	2008
Event name	ipcpSameLocalAndRemoteIp
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* remote IP address *$remoteIpAddr$* is the same as local
Cause	The local IP address and remote IP address are the same.
Effect	N/A
Recovery	No recovery is necessary.

56.6 ipv6cpPeerOnDifferentSubnet

Table 1021: ipv6cpPeerOnDifferentSubnet properties

Property name	Value
Application name	PPP
Event ID	2018
Event name	ipv6cpPeerOnDifferentSubnet
SNMP notification prefix and OID	N/A
Default severity	warning

Property name	Value
Message format string	Port *$subject$* remote Interface ID *$remoteIntId$* is not on the local subnet *$localSubnet$*
Cause	The peer is in a different subnet than us.
Effect	N/A
Recovery	No recovery is necessary.

56.7 ipv6cpPeerRejectedOurIntId

Table 1022: ipv6cpPeerRejectedOurIntId properties

Property name	Value
Application name	PPP
Event ID	2017
Event name	ipv6cpPeerRejectedOurIntId
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* local Interface ID *$localIpAddr$* negotiation rejected by remote
Cause	The peer rejected our IP address configuration request.
Effect	N/A
Recovery	No recovery is necessary.

56.8 ipv6cpPeerSuggestedDiffIntId

Table 1023: ipv6cpPeerSuggestedDiffIntId properties

Property name	Value
Application name	PPP
Event ID	2016
Event name	ipv6cpPeerSuggestedDiffIntId
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	warning
Message format string	Port *$subject$* local Interface ID *$localIpAddr$* different from Interface ID *$remoteIntId$* suggested by remote
Cause	The peer suggested a different Interface ID via a 'confnak' message.
Effect	N/A
Recovery	No recovery is necessary.

56.9 ipv6cpRemoteIntIdUnknown

Table 1024: ipv6cpRemoteIntIdUnknown properties

Property name	Value
Application name	PPP
Event ID	2014
Event name	ipv6cpRemoteIntIdUnknown
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* remote Interface ID is unknown
Cause	The remote Interface ID is unknown.
Effect	N/A
Recovery	No recovery is necessary.

56.10 ipv6cpSameLocalAndRemoteIntId

Table 1025: ipv6cpSameLocalAndRemoteIntId properties

Property name	Value
Application name	PPP
Event ID	2015
Event name	ipv6cpSameLocalAndRemoteIntId

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Port *$subject$* remote Interface ID *$remoteIntId$* is the same as local
Cause	The local and remote Interface ID's are the same.
Effect	N/A
Recovery	No recovery is necessary.

56.11 tmnxPppCpDown

Table 1026: tmnxPppCpDown properties

Property name	Value
Application name	PPP
Event ID	2002
Event name	tmnxPppCpDown
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.2
Default severity	minor
Message format string	Port *$subject$ $tmnxPppCpProtocol$* left 'opened' state
Cause	The finite state machine of a control protocol (LCP, LQR, etc.) left the OPENED state.
Effect	N/A
Recovery	N/A

56.12 tmnxPppCpUp

Table 1027: tmnxPppCpUp properties

Property name	Value
Application name	PPP
Event ID	2001

Property name	Value
Event name	tmnxPppCpUp
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.1
Default severity	minor
Message format string	Port *$subject$ $tmnxPppCpProtocol$* reached 'opened' state
Cause	The finite state machine of a control protocol (LCP, LQR, etc.) reached the OPENED state.
Effect	N/A
Recovery	N/A

56.13 tmnxPppKeepaliveFailure

Table 1028: tmnxPppKeepaliveFailure properties

Property name	Value
Application name	PPP
Event ID	2005
Event name	tmnxPppKeepaliveFailure
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.5
Default severity	minor
Message format string	Port *$subject$* PPP keepalive failed
Cause	The keepalive based on echo packets failed.
Effect	N/A
Recovery	N/A

56.14 tmnxPppLoopback

Table 1029: tmnxPppLoopback properties

Property name	Value
Application name	PPP

Property name	Value
Event ID	2012
Event name	tmnxPppLoopback
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.7
Default severity	warning
Message format string	*$tmnxPortPortID$* receiving its own magic number - channel appears to be looped back
Cause	Received the same magic number from the peer as the local magic number. The channel may be looped back.
Effect	N/A
Recovery	No recovery is necessary.

56.15 tmnxPppLoopbackClear

Table 1030: tmnxPppLoopbackClear properties

Property name	Value
Application name	PPP
Event ID	2013
Event name	tmnxPppLoopbackClear
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.8
Default severity	warning
Message format string	*$tmnxPortPortID$* channel loopback appears to be removed
Cause	The loopback condition had been cleared. It means that the value of the local magic number is different than the value of the magic number sent by the peer.
Effect	N/A
Recovery	No recovery is necessary.

56.16 tmnxPppLqmFailure

Table 1031: tmnxPppLqmFailure properties

Property name	Value
Application name	PPP
Event ID	2006
Event name	tmnxPppLqmFailure
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.6
Default severity	minor
Message format string	Port *$subject$* PPP LQM failure: LqmInRate *$tmnxPppLqmInRate$* or LqmOutRate *$tmnxPppLqmOutRate$* below PppQuality *$tmnxPpp Quality$*
Cause	The link has failed to meet the specified quality percentage.
Effect	N/A
Recovery	N/A

56.17 tmnxPppNcpDown

Table 1032: tmnxPppNcpDown properties

Property name	Value
Application name	PPP
Event ID	2004
Event name	tmnxPppNcpDown
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.4
Default severity	minor
Message format string	Port *$subject$ $tmnxPppCpProtocol$* left 'opened' state
Cause	The finite state machine of a network control protocol (IPCP, MPLSCP, BCP, OSICP, etc.) left the OPENED state.
Effect	N/A
Recovery	N/A

56.18 tmnxPppNcpUp

Table 1033: tmnxPppNcpUp properties

Property name	Value
Application name	PPP
Event ID	2003
Event name	tmnxPppNcpUp
SNMP notification prefix and OID	TIMETRA-PPP-MIB.tmnxPppNotification.3
Default severity	minor
Message format string	Port *$subject$ $tmnxPppCpProtocol$* reached 'opened' state
Cause	The finite state machine of a network control protocol (IPCP, MPLSCP, BCP, OSICP, etc.) reached the OPENED state.
Effect	N/A
Recovery	N/A

57 PPPOE

57.1 tmnxMlpppBundleIndicatorsChange

Table 1034: tmnxMlpppBundleIndicatorsChange properties

Property name	Value
Application name	PPPOE
Event ID	2003
Event name	tmnxMlpppBundleIndicatorsChange
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.3
Default severity	warning
Message format string	The value of tmnxMlpppBundleIndictors changed to *$tmnxMlpppBundleIndictors$ - $tmnxPppoeNotifyDescription$*.
Cause	The value of the object tmnxMlpppBundleIndicatorsChange has changed. A particular change is the change from 'lfi|lfiCfg' to 'lfiCfg': since interleaving is only supported on bundles with a single link, interleaving is disabled when a second link is added to a bundle.
Effect	When the value of the object tmnxMlpppBundleIndicatorsChange changes from 'lfi|lifCfg' to 'lfiCfg', Link Fragmentation and Interleaving (LFI) is disabled on the bundle.
Recovery	N/A

57.2 tmnxPppoeNcpFailure

Table 1035: tmnxPppoeNcpFailure properties

Property name	Value
Application name	PPPOE
Event ID	2002
Event name	tmnxPppoeNcpFailure
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.2

Property name	Value
Default severity	warning
Message format string	PPPoE NCP phase failure on SAP *$sapEncapValue$* in service *$svcId $ - $tmnxPppoeNcpFailureReason$*
Cause	The system could not handle a NCP phase for a PPPoE session. The problem is described in the managed object tmnxPppoeNcpFailure Reason.
Effect	N/A
Recovery	N/A

57.3 tmnxPppoeSessionFailure

Table 1036: tmnxPppoeSessionFailure properties

Property name	Value
Application name	PPPOE
Event ID	2001
Event name	tmnxPppoeSessionFailure
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.1
Default severity	warning
Message format string	PPPoE session failure on SAP *$sapEncapValue$* in service *$svcId$ - $tmnxPppoeSessionFailureReason$*
Cause	The system could not create a new PPPoE session in the tmnxPppoe SessionTable. The problem is described in the managed object tmnx PppoeSessionFailureReason.
Effect	N/A
Recovery	No recovery is necessary.

58 PTP

58.1 tmnxPtpCardNotSupported

Table 1037: tmnxPtpCardNotSupported properties

Property name	Value
Application name	PTP
Event ID	2001
Event name	tmnxPtpCardNotSupported
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.1
Default severity	minor
Message format string	CPM *$tmnxCpmCardSlotNum$* does not support IEEE1588 (PTP) operation for the configured clock-type
Cause	The tmnxPtpCardNotSupported notification is generated when the Precision Timing Protocol (PTP) is enabled on a card that is not capable of clock recovery using PTP. This notification is triggered when the TIMETRA-CHASSIS-MIB::tmnxCpmCardOscillatorType is not 'ocxo (3)', the tmnxPtpClockClockType is set to 'ordinarySlave (1)' or 'boundary (3)', and tmnxPtpClockAdminState is set to 'inService (2)'.
Effect	While this event is active, tmnxPtpClockOperState will be 'outOfService (3)' on the card that this notification was generated.
Recovery	This event is cleared when a replacement CPM card with an Oscillator of type 'ocxo (3)' is inserted. tmnxPtpCardNotSupportedClear is generated when this event is cleared.

58.2 tmnxPtpCardNotSupportedClear

Table 1038: tmnxPtpCardNotSupportedClear properties

Property name	Value
Application name	PTP
Event ID	2002

Property name	Value
Event name	tmnxPtpCardNotSupportedClear
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.2
Default severity	minor
Message format string	CPM *$tmnxCpmCardSlotNum$* supports IEEE1588 (PTP) operation for the configured clock-type
Cause	The tmnxPtpCardNotSupportedClear notification is generated when the tmnxPtpCardNotSupported event is cleared for a particular CPM card.
Effect	N/A
Recovery	N/A

58.3 tmnxPtpClockRecoveryStateChange

Table 1039: tmnxPtpClockRecoveryStateChange properties

Property name	Value
Application name	PTP
Event ID	2004
Event name	tmnxPtpClockRecoveryStateChange
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.4
Default severity	minor
Message format string	IEEE1588 (PTP) Frequency Recovery state: *$tmnxPtpClockRecovery State$*
Cause	The tmnxPtpClockRecoveryStateChange is generated when the Precision Timing Protocol (PTP) clock recovery state changes on the system.
Effect	N/A
Recovery	N/A

58.4 tmnxPtpDynamicChange

Table 1040: tmnxPtpDynamicChange properties

Property name	Value
Application name	PTP
Event ID	2007
Event name	tmnxPtpDynamicChange
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.7
Default severity	minor
Message format string	IEEE1588 (PTP) *$tmnxPtpNotifyRowDescription$*
Cause	The tmnxPtpDynamicChange notification is generated when an object dynamically (ie. Not by configuration) changes state. This notification identifies the affected row.
Effect	N/A
Recovery	N/A

58.5 tmnxPtpMasterClockChangedEvent

Table 1041: tmnxPtpMasterClockChangedEvent properties

Property name	Value
Application name	PTP
Event ID	2003
Event name	tmnxPtpMasterClockChangedEvent
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.3
Default severity	minor
Message format string	PTP Parent Clock changed. New Parent *$tmnxPtpMasterClockAddress $*, Old Parent *$tmnxPtpMasterClockLastIpAddress$*.
Cause	The tmnxPtpMasterClockChangedEvent is generated when the Master/Parent Clock for the Precision Timing Protocol (PTP) changes on the system.
Effect	N/A
Recovery	N/A

58.6 tmnxPtpOutOfResources

Table 1042: tmnxPtpOutOfResources properties

Property name	Value
Application name	PTP
Event ID	2005
Event name	tmnxPtpOutOfResources
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.5
Default severity	minor
Message format string	IEEE1588 (PTP) Card *$tmnxChassisNotifyHwIndex$* out of resources
Cause	The tmnxPtpOutOfResources notification is generated when the Precision Timing Protocol (PTP) process on the card is out of resources. This may occur in either two situations: 1. The number of PTP peers exceeds the system limit. 2. The total unicast packet rate negotiated with all PTP peers has reached the maximum packet rate supported by the system. Exceeding this rate would impact the ability of the master clock to provide an accurate stream of timing packets to each remote slave clock. If either of the two situations above occur, the PTP process will reject any new unicast packet requests from remote slave PTP peers. tmnxPtpCardOutOfResourcesClear is generated when this event is cleared.
Effect	N/A
Recovery	N/A

58.7 tmnxPtpOutOfResourcesClear

Table 1043: tmnxPtpOutOfResourcesClear properties

Property name	Value
Application name	PTP
Event ID	2006
Event name	tmnxPtpOutOfResourcesClear
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.6
Default severity	minor

Property name	Value
Message format string	IEEE1588 (PTP) Card *$tmnxChassisNotifyHwIndex$* out of resources cleared
Cause	The tmnxPtpOutOfResourcesClear notification is generated when both the total number of active PTP peers and the total negotiated unicast packet rate goes below 90% of the system limit.
Effect	N/A
Recovery	N/A

58.8 tmnxPtpPortNoTimestamping

Table 1044: tmnxPtpPortNoTimestamping properties

Property name	Value
Application name	PTP
Event ID	2008
Event name	tmnxPtpPortNoTimestamping
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.8
Default severity	minor
Message format string	Port *$tmnxPtpNotifyPortId$* does not support PTP port-based time stamping. Performance may be degraded.
Cause	The tmnxPtpPortNoTimestamping notification is generated when a PTP port is created and the associated Ethernet port does not support IEEE 1588-2008 port-based timestamping.
Effect	The PTP port is created but the performance may be degraded due to timestamping at the CPM. For optimal performance, ensure PTP is enabled on ports with IEEE 1588-2008 port-based timestamping capability.
Recovery	The Ethernet port used for the PTP port should be changed to a port on an MDA that supports IEEE 1588-2008 port-based timestamping.

59 RADIUS

59.1 tmnxRadAcctOnOngoing

Table 1045: tmnxRadAcctOnOngoing properties

Property name	Value
Application name	RADIUS
Event ID	2003
Event name	tmnxRadAcctOnOngoing
SNMP notification prefix and OID	TIMETRA-RADIUS-MIB.tmnxRadProxNotifications.3
Default severity	minor
Message format string	No reply from RADIUS server *$tmnxRadSrvPlcyName$* after *$tmnx RadSrvPlcyAcctOnOffRetryCnt$* retries *$tmnxRadiusAdditionalInfo$*
Cause	The tmnxRadAcctOnOngoing notification is sent each time the acct-on client has sent 10 RADIUS Accounting-On messages without receiving any Ack.
Effect	RADIUS is unaware that the system is online.
Recovery	The system will keep on retrying indefinitly.

59.2 tmnxRadRouteDownloadFailed

Table 1046: tmnxRadRouteDownloadFailed properties

Property name	Value
Application name	RADIUS
Event ID	2002
Event name	tmnxRadRouteDownloadFailed
SNMP notification prefix and OID	TIMETRA-RADIUS-MIB.tmnxRadProxNotifications.2
Default severity	minor
Message format string	RADIUS route download failed : *$tmnxRadiusAdditionalInfo$*

Property name	Value
Cause	The tmnxRadRouteDownloadFailed notification is sent when a RADIUS route-download process failed.
Effect	The route-download process is delayed.
Recovery	The route-download process restarts after the time defined in tmnxRad RouteDownlDownloadIntvl.

59.3 tmnxRadSrvPlcySrvOperStateCh

Table 1047: tmnxRadSrvPlcySrvOperStateCh properties

Property name	Value
Application name	RADIUS
Event ID	2001
Event name	tmnxRadSrvPlcySrvOperStateCh
SNMP notification prefix and OID	TIMETRA-RADIUS-MIB.tmnxRadProxNotifications.1
Default severity	minor
Message format string	The operational state of RADIUS server index (address= *$tmnxRadius NotifyAddr$*) in RADIUS server policy name changed to *$tmnxRadSrv PlcySrvOperState$*
Cause	The tmnxRadSrvPlcySrvOperStateCh notification is sent when the value of the object tmnxRadSrvPlcySrvOperState changes. A RADIUS server is reported as 'outOfService' when the system does not receive timely responses from that server, according to the values of the objects tmnxRadSrvPlcyTimeout and tmnxRadSrvPlcyRetry. It is reported as 'overloaded' when the system crosses the pending-requests-limit for that server.
Effect	While the value of the object tmnxRadSrvPlcySrvOperState is equal to 'outOfService' or 'overloaded', - the corresponding RADIUS server is out of use; - traffic is sent to other RADIUS server(s) associated with the same policy, depending on the value of the object tmnxRad SrvPlcyAlgorithm. - after the time specified in the object tmnxRadSrv PlcyDownTime has elapsed, the state changes to 'unknown'. While the value of the object tmnxRadSrvPlcySrvOperState is equal to 'unknown', the system sends traffic to the RADIUS server; if it replies timely, the operational state will change to 'inService', otherwise to 'outOfService'.
Recovery	The communication with the RADIUS server should recover after some time. Otherwise, or if it becomes out of use too frequently, the capacity

Property name	Value
	of the RADIUS server(s) may have to be increased, or the values of the objects mentioned above may have to be adapted.

60 RIP

60.1 ripPacketDiscarded

Table 1048: ripPacketDiscarded properties

Property name	Value
Application name	RIP
Event ID	2001
Event name	ripPacketDiscarded
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Discarded packet from *$ripPacketSrcIp$* because *$ripPacketDiscardReason$*
Cause	The following checks are performed on an incoming RIP packet - valid RIP version - valid source address and port - valid destination address and port - valid AF_INET field - valid command field - valid routes etc. If a packet fails any of these checks it must be discarded, and the event is logged
Effect	N/A
Recovery	N/A

60.2 vRtrRipAuthTypeFailure

Table 1049: vRtrRipAuthTypeFailure properties

Property name	Value
Application name	RIP
Event ID	2003
Event name	vRtrRipAuthTypeFailure
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.2
Default severity	minor

Property name	Value
Message format string	Authentication type failure on packet received on interface *$vRtrRip PeerIfIndex$* from peer *$vRtrRipPeerAddress$*
Cause	The authentication key in a received RIPv2 packet conflicted with the authentication key configured for this router.
Effect	N/A
Recovery	N/A

60.3 vRtrRipAuthTypeMismatch

Table 1050: vRtrRipAuthTypeMismatch properties

Property name	Value
Application name	RIP
Event ID	2002
Event name	vRtrRipAuthTypeMismatch
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.1
Default severity	minor
Message format string	Authentication type mismatch on packet received on interface *$vRtrRip PeerIfIndex$* from peer *$vRtrRipPeerAddress$*
Cause	The authentication type field in a received RIPv2 packet conflicted with the authentication type configured for this router.
Effect	N/A
Recovery	N/A

60.4 vRtrRipInstanceExpLmtReached

Table 1051: vRtrRipInstanceExpLmtReached properties

Property name	Value
Application name	RIP
Event ID	2006
Event name	vRtrRipInstanceExpLmtReached

Property name	Value
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.5
Default severity	major
Message format string	RIP instance *$vRtrID$* has reached the export-limit *$vRtrRipInstance ExportLimit$*, additional routes will not be exported into RIP
Cause	RIP instance has exported maximum allowed export routes. It will not export any more routes unless the export policy and export limit is changed.
Effect	RIP will not export any more routes.
Recovery	Change RIP export policy.

60.5 vRtrRipInstanceExpLmtWarning

Table 1052: vRtrRipInstanceExpLmtWarning properties

Property name	Value
Application name	RIP
Event ID	2007
Event name	vRtrRipInstanceExpLmtWarning
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.6
Default severity	warning
Message format string	RIP instance *$vRtrID$* has reached *$vRtrRipInstanceExpLmtLog Percent$* percent of the export limit *$vRtrRipInstanceExportLimit$*
Cause	The number of routes exported by RIP has reached the warning percent of the configured export limit. RIP will continue to export routes till the limit is reached.
Effect	N/A
Recovery	N/A

60.6 vRtrRipInstanceRestarted

Table 1053: vRtrRipInstanceRestarted properties

Property name	Value
Application name	RIP
Event ID	2005
Event name	vRtrRipInstanceRestarted
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.4
Default severity	major
Message format string	Instance *$vRtrID$* restarted
Cause	The RIP instance has restarted. When a RIP protocol instance runs out of resources, the instance shuts down and then attempts to restart within 30 seconds.
Effect	N/A
Recovery	N/A

60.7 vRtrRipInstanceRtsExpLmtDropped

Table 1054: vRtrRipInstanceRtsExpLmtDropped properties

Property name	Value
Application name	RIP
Event ID	2008
Event name	vRtrRipInstanceRtsExpLmtDropped
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.7
Default severity	warning
Message format string	The number of redistributed routes into RIP has dropped below the export limit *$vRtrRipInstanceExportLimit$*
Cause	Number of exported routes is dropped below the configured export limit.
Effect	N/A
Recovery	N/A

60.8 vRtrRipInstanceShuttingDown

Table 1055: vRtrRipInstanceShuttingDown properties

Property name	Value
Application name	RIP
Event ID	2004
Event name	vRtrRipInstanceShuttingDown
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.3
Default severity	major
Message format string	Instance *$vRtrID$* is being operationally 'shutdown' because *$rip InstanceShuttingDownReason$*
Cause	The RIP instance shut down on its own accord when the protocol ran out of resources such as memory.
Effect	N/A
Recovery	The instance will attempt to restart within 30 seconds of shutting down.

61 RIP_NG

61.1 tmnxRipNgAuthFailure

Table 1056: tmnxRipNgAuthFailure properties

Property name	Value
Application name	RIP_NG
Event ID	2003
Event name	tmnxRipNgAuthFailure
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.2
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgAuthFailure trap is generated when the authentication key in a received RIPv2 packet conflicts with the authentication key configured for this router.
Effect	N/A
Recovery	N/A

61.2 tmnxRipNgAuthTypeMismatch

Table 1057: tmnxRipNgAuthTypeMismatch properties

Property name	Value
Application name	RIP_NG
Event ID	2002
Event name	tmnxRipNgAuthTypeMismatch
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.1
Default severity	minor
Message format string	TODO

Property name	Value
Cause	A tmnxRipNgAuthTypeMismatch trap is generated when the authentication type field in a received RIPv2 packet conflicts with the authentication type configured for this router.
Effect	N/A
Recovery	N/A

61.3 tmnxRipNgIfUcastAddrNotUsed

Table 1058: tmnxRipNgIfUcastAddrNotUsed properties

Property name	Value
Application name	RIP_NG
Event ID	2009
Event name	tmnxRipNgIfUcastAddrNotUsed
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.8
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgIfUcastAddrNotUsed notification is generated when a neighbor has one or more unicast-addresses configured but it's send mode is not set to 'unicast'.
Effect	N/A
Recovery	N/A

61.4 tmnxRipNgInstExpLmtReached

Table 1059: tmnxRipNgInstExpLmtReached properties

Property name	Value
Application name	RIP_NG
Event ID	2006
Event name	tmnxRipNgInstExpLmtReached
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.5

Property name	Value
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgInstExpLmtReached notification is generated when the configured value of exported routes, tmnxRipNgInstExportLimit is reached. Additional routes would not be exported into RIP/RIP-NG from the route table.
Effect	N/A
Recovery	N/A

61.5 tmnxRipNgInstExpLmtWarning

Table 1060: tmnxRipNgInstExpLmtWarning properties

Property name	Value
Application name	RIP_NG
Event ID	2007
Event name	tmnxRipNgInstExpLmtWarning
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.6
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgInstExpLmtWarning notification is generated when the number of exported routes is equal to the configured percent, tmnxRip NgInstExpLmtLogPct of the export limit, tmnxRipNgInstExportLimit. Additional routes will continue to be exported into RIP/RIP-NG from the route table till the export limit is reached.
Effect	N/A
Recovery	N/A

61.6 tmnxRipNgInstRestarted

Table 1061: tmnxRipNgInstRestarted properties

Property name	Value
Application name	RIP_NG
Event ID	2005
Event name	tmnxRipNgInstRestarted
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.4
Default severity	minor
Message format string	TODO
Cause	When a RIP/RIP-NG protocol instance runs out of resources, the instance will shut down and then attempt to restart within 30 seconds. A tmnxRipNgInstRestarted trap is generated when the RIP instance has restarted.
Effect	N/A
Recovery	N/A

61.7 tmnxRipNgInstRtsExpLmtDropped

Table 1062: tmnxRipNgInstRtsExpLmtDropped properties

Property name	Value
Application name	RIP_NG
Event ID	2008
Event name	tmnxRipNgInstRtsExpLmtDropped
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.7
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgInstRtsExpLmtDropped notification is generated when the number of exported routes drops below the export limit, tmnxRipNgInstExportLimit.
Effect	N/A
Recovery	N/A

61.8 tmnxRipNgInstShuttingDown

Table 1063: tmnxRipNgInstShuttingDown properties

Property name	Value
Application name	RIP_NG
Event ID	2004
Event name	tmnxRipNgInstShuttingDown
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.3
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgInstShuttingDown trap is generated when the RIP/RIP-NG instance shuts down on its own accord when the protocol runs out of resources such as memory. The instance will attempt to restart within 30 seconds of shutting down.
Effect	N/A
Recovery	N/A

61.9 tmnxRipNgPacketDiscarded

Table 1064: tmnxRipNgPacketDiscarded properties

Property name	Value
Application name	RIP_NG
Event ID	2001
Event name	tmnxRipNgPacketDiscarded
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.1
Default severity	minor
Message format string	TODO
Cause	A tmnxRipNgPacketDiscarded trap is generated when a RIP/RIP-NG packet is discarded for this router.
Effect	N/A

Property name	Value
Recovery	N/A

62 ROUTE_POLICY

62.1 trigPolicyPrevEval

Table 1065: trigPolicyPrevEval properties

Property name	Value
Application name	ROUTE_POLICY
Event ID	2001
Event name	trigPolicyPrevEval
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Triggered policy is enabled - protocol re-evaluation must be triggered manually
Cause	A triggered policy was enabled.
Effect	N/A
Recovery	A protocol re-evaluation must be triggered manually.

63 RPKI

63.1 tmnxRpkiNotifySession

Table 1066: tmnxRpkiNotifySession properties

Property name	Value
Application name	RPKI
Event ID	2001
Event name	tmnxRpkiNotifySession
SNMP notification prefix and OID	TIMETRA-RPKI-MIB.tmnxRpkiNotifications.1
Default severity	minor
Message format string	Rpki Session state on *$tmnxRpkiPeerAddr$* changed to *$tmnxRpkiTrapStatus$* due to *$tmnxRpkiErrorType$*
Cause	A tmnxRpkiNotifySession notification is generated when a rpki session either comes up or goes down. Possible reasons for this to happen is listed below: (a) a session goes down due to hold-timer expiry. (b) a session goes down due to failure of the TCP connection. (c) a session goes down due to session ID mismatch. (d) a session goes down due to sent or received Error Report PDU containing fatal error code (e) a session comes up (established state)
Effect	This may remove the routes learnt from a particular rpki server if session goes down. Or start learning routes from a rpki session which was newly established.
Recovery	There is no recovery required for this notification.

63.2 tmnxRpkiStaleTimerExpiry

Table 1067: tmnxRpkiStaleTimerExpiry properties

Property name	Value
Application name	RPKI
Event ID	2002

Property name	Value
Event name	tmnxRpkiStaleTimerExpiry
SNMP notification prefix and OID	TIMETRA-RPKI-MIB.tmnxRpkiNotifications.2
Default severity	minor
Message format string	Stale timer Expired for the Rpki session : *$tmnxRpkiPeerAddr$*
Cause	This notification is generated when a stale timer expires. The stale timer expires due to the following reasons: 1) The peer goes down, and never comes up within the stale timer interval 2) Peer goes down and comes backup and refreshes the databases. The stale timer is expired to remove unrefreshed entries in the database. 3) The peer goes down and comes back again and again goes down before refreshing any entries. Here again the stale timer is expired due to unstable connection.
Effect	This may remove the routes learnt from a particular rpki server if session goes down. Or start learning routes from a rpki session which was newly established.
Recovery	There is no recovery required for this notification.

64 RSVP

64.1 vRtrRsvpIfNbrStateDown

Table 1068: vRtrRsvpIfNbrStateDown properties

Property name	Value
Application name	RSVP
Event ID	2004
Event name	vRtrRsvpIfNbrStateDown
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.4
Default severity	warning
Message format string	Neighbor *$vRtrRsvpNbrAddress$* on interface *$ifIndex$* changed to inactive state because *$vRtrRsvpIfNbrDownReasonCode$*
Cause	A RSVP interface neighbor changed to the inactive state.
Effect	N/A
Recovery	N/A

64.2 vRtrRsvpIfNbrStateUp

Table 1069: vRtrRsvpIfNbrStateUp properties

Property name	Value
Application name	RSVP
Event ID	2003
Event name	vRtrRsvpIfNbrStateUp
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.3
Default severity	warning
Message format string	Neighbor *$vRtrRsvpNbrAddress$* on interface *$ifIndex$* changed to active state

Property name	Value
Cause	A RSVP interface neighbor changed to the active state.
Effect	N/A
Recovery	N/A

64.3 vRtrRsvpIfStateChange

Table 1070: vRtrRsvpIfStateChange properties

Property name	Value
Application name	RSVP
Event ID	2002
Event name	vRtrRsvpIfStateChange
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.2
Default severity	warning
Message format string	Interface *$ifIndex$* is in administrative state *$rsvpIfEnabled$*, operational state *$vRtrRsvpIfOperState$*
Cause	A RSVP interface changed state.
Effect	Service is affected.
Recovery	No recovery is required.

64.4 vRtrRsvpPEFailOverPriToStdBy

Table 1071: vRtrRsvpPEFailOverPriToStdBy properties

Property name	Value
Application name	RSVP
Event ID	2005
Event name	vRtrRsvpPEFailOverPriToStdBy
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.5
Default severity	warning

Property name	Value
Message format string	Traffic switched for MVPN instance *$vRtrID$* from primary PE *$vRtrPimNgMvpnUMHPEAddr$* to standby PE *$vRtrPim NgMvpnUMHPEStandbyAddr$* due to *$vRtrRsvpPEFailOverReason Code$*
Cause	The vRtrRsvpPEFailOverPriToStdBy notification is raised when primary Provider Edge (PE) has switched over to standby PE. The IP address of the primary PE can be extracted from the vRtrPim NgMvpnUMHPEAddrType and vRtrPimNgMvpnUMHPEAddr indexes of the varbinds in this notification.
Effect	The tunnel traffic may be affected.
Recovery	None required.

64.5 vRtrRsvpPEFailOverStdByToPri

Table 1072: vRtrRsvpPEFailOverStdByToPri properties

Property name	Value
Application name	RSVP
Event ID	2006
Event name	vRtrRsvpPEFailOverStdByToPri
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.6
Default severity	minor
Message format string	Traffic switched for MVPN instance *$vRtrID$* from standby PE *$v RtrPimNgMvpnUMHPEStandbyAddr$* to primary PE *$vRtrPim NgMvpnUMHPEAddr$*
Cause	The vRtrRsvpPEFailOverPriToStdBy notification is raised when standby Provider Edge (PE) has switched over to primary PE. The IP address of the primary PE can be extracted from the vRtrPim NgMvpnUMHPEAddrType and vRtrPimNgMvpnUMHPEAddr indexes of the varbinds in this notification.
Effect	The tunnel traffic may be affected.
Recovery	None required.

64.6 vRtrRsvpStateChange

Table 1073: vRtrRsvpStateChange properties

Property name	Value
Application name	RSVP
Event ID	2001
Event name	vRtrRsvpStateChange
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.1
Default severity	warning
Message format string	Instance is in administrative state *$vRtrRsvpGeneralAdminState$*, operational state *$vRtrRsvpGeneralOperState$*
Cause	The RSVP module changed state.
Effect	Service is affected.
Recovery	No recovery is required.

65 SATELLITE

65.1 tmnxSatelliteOperStateChange

Table 1074: tmnxSatelliteOperStateChange properties

Property name	Value
Application name	SATELLITE
Event ID	2001
Event name	tmnxSatelliteOperStateChange
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.1
Default severity	minor
Message format string	Possible messages: • *$tmnxHwIndex$* is in *$tmnxHwOperState$* state - *$tmnxSatNotifyFailureReason$* • *$tmnxHwIndex$* is in *$tmnxHwOperState$* state
Cause	The tmnxSatelliteOperStateChange notification is generated when there is a change in tmnxHwOperState for the satellite.
Effect	The satellite has changed states. The tmnxSatNotifyFailureReason is only valid when tmnxHwOperState is 'failed (5)', and should otherwise be blank.
Recovery	Contact Nokia customer support if tmnxSatNotifyFailureReason does not provide enough information to rectify the situation.

65.2 tmnxSatSyncIfTimHoldover

Table 1075: tmnxSatSyncIfTimHoldover properties

Property name	Value
Application name	SATELLITE
Event ID	2006
Event name	tmnxSatSyncIfTimHoldover

Property name	Value
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.6
Default severity	critical
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$* is in holdover state
Cause	The tmnxSatSyncIfTimHoldover notification is generated when the synchronous equipment timing subsystem of the satellite transitions into a holdover state.
Effect	The transmit timing of all synchronous interfaces on the satellite are no longer synchronous with the host. This could result in traffic loss.
Recovery	Investigate the state of the two input timing references on the satellite and the links between the host and the satellite (i.e. the uplinks) that drive them for failures.

65.3 tmnxSatSyncIfTimHoldoverClear

Table 1076: tmnxSatSyncIfTimHoldoverClear properties

Property name	Value
Application name	SATELLITE
Event ID	2007
Event name	tmnxSatSyncIfTimHoldoverClear
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.7
Default severity	cleared
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$*, holdover state cleared
Cause	The tmnxSatSyncIfTimHoldoverClear notification is generated when the synchronous equipment timing subsystem of the satellite transitions out of the holdover state.
Effect	This notification is for informational purposes only.
Recovery	No recovery required.

65.4 tmnxSatSyncIfTimRef1Alarm

Table 1077: tmnxSatSyncIfTimRef1Alarm properties

Property name	Value
Application name	SATELLITE
Event ID	2008
Event name	tmnxSatSyncIfTimRef1Alarm
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.8
Default severity	minor
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$*, alarm *$tmnxSatNotifySyncIfTimRefAlarm$* on reference 1
Cause	The tmnxSatSyncIfTimRef1Alarm notification is generated when an alarm condition on the first timing reference is detected.
Effect	If the other timing reference is free of faults, the satellite no longer has a backup timing reference. If the other timing reference also has a fault, the satellite will likely no longer be synchronous with the host.
Recovery	Investigate the state of the link between the host and the satellite (i.e. the uplink) that drives the first timing reference on the satellite for faults.

65.5 tmnxSatSyncIfTimRef1AlarmClear

Table 1078: tmnxSatSyncIfTimRef1AlarmClear properties

Property name	Value
Application name	SATELLITE
Event ID	2009
Event name	tmnxSatSyncIfTimRef1AlarmClear
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.9
Default severity	cleared
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$*, alarm *$tmnxSatNotifySyncIfTimRefAlarm$* on reference 1 cleared
Cause	The tmnxSatSyncIfTimRef1AlarmClear notification is generated when the alarm condition on the first timing reference is cleared.
Effect	This notification is for informational purposes only.

Property name	Value
Recovery	No recovery required.

65.6 tmnxSatSyncIfTimRef1Quality

Table 1079: tmnxSatSyncIfTimRef1Quality properties

Property name	Value
Application name	SATELLITE
Event ID	2004
Event name	tmnxSatSyncIfTimRef1Quality
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.4
Default severity	minor
Message format string	Synchronous timing interface on satellite *$tmnxSatId$*, reference 1 received quality level *$tmnxSatSyncIfTimingRef1RxQltyLvl$*
Cause	The tmnxSatSyncIfTimRef1Quality notification is generated when the received quality level changes on the first timing reference of the satellite.
Effect	This notification is for informational purposes only.
Recovery	No recovery required.

65.7 tmnxSatSyncIfTimRef2Alarm

Table 1080: tmnxSatSyncIfTimRef2Alarm properties

Property name	Value
Application name	SATELLITE
Event ID	2010
Event name	tmnxSatSyncIfTimRef2Alarm
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.10
Default severity	minor
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$*, alarm *$tmnxSatNotifySyncIfTimRefAlarm$* on reference 2

Property name	Value
Cause	The tmnxSatSyncIfTimRef2Alarm notification is generated when an alarm condition on the second timing reference is detected.
Effect	If the other timing reference is free of faults, the satellite no longer has a backup timing reference. If the other timing reference also has a fault, the satellite will likely no longer be synchronous with the host.
Recovery	Investigate the state of the link between the host and the satellite (i.e. the uplink) that drives the second timing reference on the satellite for faults.

65.8 tmnxSatSyncIfTimRef2AlarmClear

Table 1081: tmnxSatSyncIfTimRef2AlarmClear properties

Property name	Value
Application name	SATELLITE
Event ID	2011
Event name	tmnxSatSyncIfTimRef2AlarmClear
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.11
Default severity	cleared
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$*, alarm *$tmnxSatNotifySyncIfTimRefAlarm$* on reference 2 cleared
Cause	The tmnxSatSyncIfTimRef1AlarmClear notification is generated when the alarm condition on the second timing reference is cleared.
Effect	This notification is for informational purposes only.
Recovery	No recovery required.

65.9 tmnxSatSyncIfTimRef2Quality

Table 1082: tmnxSatSyncIfTimRef2Quality properties

Property name	Value
Application name	SATELLITE
Event ID	2005

Property name	Value
Event name	tmnxSatSyncIfTimRef2Quality
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.5
Default severity	minor
Message format string	Synchronous timing interface on satellite *$tmnxSatId$*, reference 2 received quality level *$tmnxSatSyncIfTimingRef2RxQltyLvl$*
Cause	The tmnxSatSyncIfTimRef2Quality notification is generated when the received quality level changes on the second timing reference of the satellite.
Effect	This notification is for informational purposes only.
Recovery	No recovery required.

65.10 tmnxSatSyncIfTimRefSwitch

Table 1083: tmnxSatSyncIfTimRefSwitch properties

Property name	Value
Application name	SATELLITE
Event ID	2002
Event name	tmnxSatSyncIfTimRefSwitch
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.2
Default severity	minor
Message format string	Synchronous timing interface on satellite *$tmnxSatId$*, timing reference changed to *$tmnxSatSyncIfTimingRef1InUse$*
Cause	The tmnxSatSyncIfTimRefSwitch notification is generated when there is a change of which timing reference is providing timing for the satellite.
Effect	This event is for notification only.
Recovery	No recovery required.

65.11 tmnxSatSyncIfTimSystemQuality

Table 1084: tmnxSatSyncIfTimSystemQuality properties

Property name	Value
Application name	SATELLITE
Event ID	2003
Event name	tmnxSatSyncIfTimSystemQuality
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.3
Default severity	minor
Message format string	Synchronous timing interface on satellite *$tmnxSatId$*, system quality level changed to *$tmnxSatSyncIfTimingSystemQltyLvl$*
Cause	This notification may be triggered for the following reasons: 1) There has been a switch in the timing reference in use by the network element, either because the previously active timing reference was disqualified, or to ensure that the network element is using the timing reference with the best timing quality. 2) There has been a change in the active timing reference's quality and the change does not result in a timing reference switch. 3) The network element has transitioned into or out of the holdover state.
Effect	The system quality level is used to determine the SSM code transmitted on synchronous interfaces. This may affect the SSM code transmitted on some or all interfaces, which may affect the distribution of timing throughout the network.
Recovery	If the customer is expecting the system to be locked to a reference of a particular quality and the system quality has decreased, the customer will need to determine the root cause (for example, loss of communication with a satellite) and resolve the issue.

66 SECURITY

66.1 cli_user_login

Table 1085: cli_user_login properties

Property name	Value
Application name	SECURITY
Event ID	2001
Event name	cli_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required

66.2 cli_user_login_failed

Table 1086: cli_user_login_failed properties

Property name	Value
Application name	SECURITY
Event ID	2003
Event name	cli_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	A user failed authentication.

Property name	Value
Effect	The user access session does not begin. The user will be given another opportunity to authenticate himself.
Recovery	No recovery is required

66.3 cli_user_login_max_attempts

Table 1087: cli_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2004
Event name	cli_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.46
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxUserCliLoginMaxAttempts notification is generated when a user attempting to open a CLI sesssion failed to authenticate for more than a maximum allowed number of times in a period of tmnxPassword AttemptsTime minutes. The value of the object tmnxPasswordAttempts Count indicates the maximum number of unsuccessful login attempts allowed. The value of the object tmnxPasswordAttemptsLockout Period indicates the number of minutes the user is locked out if the threshold of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUserName indicates the name of the user attempting to open a CLI session. The value of the object tmnx SecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to open a CLI session.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. A remote access session is terminated.
Recovery	No recovery action is required.

66.4 cli_user_logout

Table 1088: cli_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2002
Event name	cli_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	A user access session ended.
Recovery	No recovery is required

66.5 enable_admin

Table 1089: enable_admin properties

Property name	Value
Application name	SECURITY
Event ID	2022
Event name	enable_admin
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	User *$userName$* from *$srcAddr$* successfully entered into admin enable mode
Cause	A user successfully entered into the admin enable mode.
Effect	A user access session is started.
Recovery	No recovery is required

66.6 enable_admin_failed

Table 1090: enable_admin_failed properties

Property name	Value
Application name	SECURITY
Event ID	2241
Event name	enable_admin_failed
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	User *$userName$* from *$srcAddr$* failed to enter admin enable mode
Cause	A user failed to enter the admin enable mode.
Effect	N/A
Recovery	No recovery is required

66.7 ftp_transfer_failed

Table 1091: ftp_transfer_failed properties

Property name	Value
Application name	SECURITY
Event ID	2021
Event name	ftp_transfer_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	*$appType$* of *$fileName$* initiated by *$userName$* from *$srcAddr$* to *$dstAddr$* failed.
Cause	A FTP/TFTP transfer failed.
Effect	N/A
Recovery	No recovery is required

66.8 ftp_transfer_successful

Table 1092: ftp_transfer_successful properties

Property name	Value
Application name	SECURITY
Event ID	2020
Event name	ftp_transfer_successful
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	*$appType$* of *$fileName$* initiated by *$userName$* from *$srcAddr$* to *$dstAddr$* completed successfully.
Cause	A FTP/TFTP transfer completed successfully.
Effect	N/A
Recovery	No recovery is required

66.9 ftp_user_login

Table 1093: ftp_user_login properties

Property name	Value
Application name	SECURITY
Event ID	2005
Event name	ftp_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	A user was successfully authenticated for login.
Effect	A user access session was started
Recovery	No recovery is required

66.10 ftp_user_login_failed

Table 1094: ftp_user_login_failed properties

Property name	Value
Application name	SECURITY
Event ID	2007
Event name	ftp_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session was not started. The user will be given another opportunity to authenticate himself.
Recovery	No recovery is required

66.11 ftp_user_login_max_attempts

Table 1095: ftp_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2008
Event name	ftp_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.47
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxUserFtpLoginMaxAttempts notification is generated when a user attempting to connect via FTP failed to authenticate for more than a maximum allowed number of times in a period of tmnxPassword AttemptsTime minutes. The value of the object tmnxPasswordAttempts Count indicates the maximum number of unsuccessful login attempts allowed. The value of the object tmnxPasswordAttemptsLockoutPeriod indicates the number of minutes the user is locked out if the threshold

Property name	Value
	of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUserName indicates the name of the user attempting to connect via FTP. The value of the object tmnxSecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to connect via FTP.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockoutPeriod minutes. An FTP session is terminated.
Recovery	No recovery action is required.

66.12 ftp_user_logout

Table 1096: ftp_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2006
Event name	ftp_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

66.13 host_snmp_attempts

Table 1097: host_snmp_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2023
Event name	host_snmp_attempts

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	warning
Message format string	Host *$hostAddress$* is locked out for *$lockoutTime$* minutes since it exceeded the configured threshold of unsuccessful SNMP connection attempts.
Cause	The remont SNMP host exceded the configured attempts.
Effect	The remote SNMP host is locked out and the router will not respond to further SNMP requests from the host.
Recovery	N/A

66.14 mafEntryMatch

Table 1098: mafEntryMatch properties

Property name	Value
Application name	SECURITY
Event ID	2019
Event name	mafEntryMatch
SNMP notification prefix and OID	N/A
Default severity	major
Message format string	Description: *$mafEntryDescription$* .There have been *$mafEntryDropped$* matches since the previously logged match. Interface: *$sourceInterface$*, action: *$mafEntryAction$* *$mafEntryProtocol$*
Cause	A match has been found for an entry in the management access filter.
Effect	N/A
Recovery	No recovery is necessary.

66.15 mct_user_login

Table 1099: mct_user_login properties

Property name	Value
Application name	SECURITY
Event ID	2035
Event name	mct_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User *$userName$* from *$srcAddr$* logged in
Cause	A user successfully authenticated for login via MCT.
Effect	A user access session was started.
Recovery	No recovery is required.

66.16 mct_user_login_failed

Table 1100: mct_user_login_failed properties

Property name	Value
Application name	SECURITY
Event ID	2037
Event name	mct_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User *$userName$* from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session was not started. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

66.17 mct_user_login_max_attempts

Table 1101: mct_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2038
Event name	mct_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User $userName $from *$srcAddr$* attempted more than *$max Attempts$* times to log in
Cause	A user failed to authenticate in more than the permitted number of retries.
Effect	No effect.
Recovery	No recovery is required.

66.18 mct_user_logout

Table 1102: mct_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2036
Event name	mct_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out from MCT.
Effect	The user access session ended.
Recovery	No recovery is required.

66.19 netconf_user_login

Table 1103: netconf_user_login properties

Property name	Value
Application name	SECURITY
Event ID	2121
Event name	netconf_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required

66.20 netconf_user_login_failed

Table 1104: netconf_user_login_failed properties

Property name	Value
Application name	SECURITY
Event ID	2123
Event name	netconf_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session does not begin. The user will be given another opportunity to authenticate himself.
Recovery	No recovery is required

66.21 netconf_user_login_max_attempts

Table 1105: netconf_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2124
Event name	netconf_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.55
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxUserNetconfLoginMaxAttempts notification is generated when a user attempting to open a netconf session failed to authenticate for more than a maximum allowed number of times in a period of tmnxPasswordAttemptsTime minutes. The value of the object tmnxPasswordAttemptsCount indicates the maximum number of unsuccessful login attempts allowed. The value of the object tmnx PasswordAttemptsLockoutPeriod indicates the number of minutes the user is locked out if the threshold of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUserName indicates the name of the user attempting to open a netconf session. The value of the object tmnxSecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to open a netconf session.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. A remote access session is terminated.
Recovery	No recovery action is required.

66.22 netconf_user_logout

Table 1106: netconf_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2122
Event name	netconf_user_logout

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	A user access session ended.
Recovery	No recovery is required

66.23 radiusInetServerOperStatusChange

Table 1107: radiusInetServerOperStatusChange properties

Property name	Value
Application name	SECURITY
Event ID	2026
Event name	radiusInetServerOperStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.36
Default severity	minor
Message format string	RADIUS server *$radiusServerInetAddress$* operational status changed to *$radiusServerOperStatus$*.
Cause	The operational status of a RADIUS server has transitioned either from 'up' to 'down' or from 'down' to 'up'.
Effect	N/A
Recovery	No recovery is necessary.

66.24 radiusOperStatusChange

Table 1108: radiusOperStatusChange properties

Property name	Value
Application name	SECURITY
Event ID	2014

Property name	Value
Event name	radiusOperStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.7
Default severity	minor
Message format string	RADIUS operational status changed to *$radiusOperStatus$*
Cause	The radiusOperStatus has transitioned either from 'up' to 'down' or from 'down' to 'up'.
Effect	N/A
Recovery	No recovery is necessary.

66.25 radiusSystemIpAddrNotSet

Table 1109: radiusSystemIpAddrNotSet properties

Property name	Value
Application name	SECURITY
Event ID	2016
Event name	radiusSystemIpAddrNotSet
SNMP notification prefix and OID	N/A
Default severity	major
Message format string	System IP address is not configured
Cause	A user attempted authentication through RADIUS but the system IP address is not configured.
Effect	Cannot authenticate the user using RADIUS.
Recovery	Configure the system IP address.

66.26 sapDcpDynamicConform

Table 1110: sapDcpDynamicConform properties

Property name	Value
Application name	SECURITY

Property name	Value
Event ID	2059
Event name	sapDcpDynamicConform
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.446
Default severity	warning
Message format string	Sap *$sapEncapValue$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* newly conformant at *$sapDcpTimeEventOccured$*. Policy *$sapDCpu ProtPolicy$*. Policer=*$sapDcpFpProtocol$*(dynamic). Excd count= *$sap DcpFpDynExcdCount$*
Cause	The sapDcpDynamicConform notification is generated when the protocol for a particular SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected SAP is now in conformance with the parameters configured for the associated distributed CPU protection policy.
Recovery	There is no recovery required for this notification.

66.27 sapDcpDynamicEnforceAlloc

Table 1111: sapDcpDynamicEnforceAlloc properties

Property name	Value
Application name	SECURITY
Event ID	2064
Event name	sapDcpDynamicEnforceAlloc
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.51
Default severity	warning
Message format string	Dynamic *$sapDcpFpProtocol$* policers allocated for sap *$sapEncap Value$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$sapDcpTime EventOccured$*. Policy *$sapDCpuProtPolicy$*.
Cause	The sapDcpDynamicEnforceAlloc notification is generated when a dynamic enforcement policer is allocated on a particular SAP. This notification is generated when TIMETRA-SECURITY-

Property name	Value
	MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The affected SAP is not in conformance with the configured parameters of the associated distributed CPU protection policy and may be using more resources than expected and cause the system to under-perform.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.

66.28 sapDcpDynamicEnforceFreed

Table 1112: sapDcpDynamicEnforceFreed properties

Property name	Value
Application name	SECURITY
Event ID	2065
Event name	sapDcpDynamicEnforceFreed
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.52
Default severity	warning
Message format string	Dynamic *$sapDcpFpProtocol$* policers freed for sap *$sapEncapValue $* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$sapDcpTimeEvent Occured$*. Policy *$sapDCpuProtPolicy$*. Excd count= *$sapDcpFpDyn ExcdCount$*
Cause	The sapDcpDynamicEnforceFreed notification is generated when a dynamic enforcement policer is freed on a particular SAP. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The affected SAP is now in conformance with the configured parameters of the associated distributed CPU protection policy.
Recovery	There is no recovery required for this notification.

66.29 sapDcpDynamicExcd

Table 1113: sapDcpDynamicExcd properties

Property name	Value
Application name	SECURITY
Event ID	2053
Event name	sapDcpDynamicExcd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.40
Default severity	warning
Message format string	Non conformant sap *$sapEncapValue$* on fp *$tmnxCardSlotNum $*/*$tmnxFPNum$* detected at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProtPolicy$*. Policer= *$sapDcpFpProtocol$*(dynamic). Excd count=*$sapDcpFpDynExcdCount$*
Cause	The sapDcpDynamicExcd notification is generated when the protocol on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected SAP may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.

66.30 sapDcpDynamicHoldDownEnd

Table 1114: sapDcpDynamicHoldDownEnd properties

Property name	Value
Application name	SECURITY
Event ID	2057
Event name	sapDcpDynamicHoldDownEnd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.44
Default severity	warning

Property name	Value
Message format string	Hold-down completed for sap *$sapEncapValue$* on fp *$tmnxCard SlotNum$*/*$tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProtPolicy$*. Policer= *$sapDcpFpProtocol$*(dynamic). Excd count=*$sapDcpFpDynExcdCount$*
Cause	The sapDcpDynamicHoldDownEnd notification is generated when a particular SAP completes hold-down period for an exceeding protocol. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The protocol for an affected SAP will transition to a detection-time countdown after the hold-down period is complete.
Recovery	There is no recovery required for this notification.

66.31 sapDcpDynamicHoldDownStart

Table 1115: sapDcpDynamicHoldDownStart properties

Property name	Value
Application name	SECURITY
Event ID	2055
Event name	sapDcpDynamicHoldDownStart
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.42
Default severity	warning
Message format string	Hold-down started for sap *$sapEncapValue$* on fp *$tmnxCardSlotNum $*/*$tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpu ProtPolicy$*. Policer= *$sapDcpFpProtocol$*(dynamic). Excd count=*$sap DcpFpDynExcdCount$*
Cause	The sapDcpDynamicHoldDownStart notification is generated when a particular SAP starts hold-down period for an exceeding protocol. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The protocol will treat all packets as non-conformant during the hold-down period.
Recovery	There is no recovery required for this notification.

66.32 sapDcpLocMonExcd

Table 1116: sapDcpLocMonExcd properties

Property name	Value
Application name	SECURITY
Event ID	2060
Event name	sapDcpLocMonExcd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.47
Default severity	warning
Message format string	Local monitor *$sapDcpFpLocMonPlcrName$* for sap *$sapEncap Value$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* detected as non-conformant at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProt Policy$*. Excd count=*$sapDcpFpLocMonExcdCount$*
Cause	The sapDcpLocMonExcd notification is generated when the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dymanic enforcement policers. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLocMonPlcrLog Event is configured to 'verbose'.
Effect	The affected SAP may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.

66.33 sapDcpLocMonExcdAllDynAlloc

Table 1117: sapDcpLocMonExcdAllDynAlloc properties

Property name	Value
Application name	SECURITY
Event ID	2062
Event name	sapDcpLocMonExcdAllDynAlloc
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.49
Default severity	warning

Property name	Value
Message format string	All dynamic policers allocated for local monitor *$sapDcpFpLocMon PlcrName$* for sap *$sapEncapValue$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProt Policy$*. Excd count= *$sapDcpFpLocMonExcdCount$*
Cause	The sapDcpLocMonExcdAllDynAlloc notification is generated when all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for a particular SAP. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLocMonPlcrLogEvent is configure to 'verbose'.
Effect	The affected SAP may be using more resources than expected and cause the system to under-perform.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.

66.34 sapDcpLocMonExcdAllDynFreed

Table 1118: sapDcpLocMonExcdAllDynFreed properties

Property name	Value
Application name	SECURITY
Event ID	2063
Event name	sapDcpLocMonExcdAllDynFreed
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.50
Default severity	warning
Message format string	All dynamic policers freed for local monitor *$sapDcpFpLocMon PlcrName$* for sap *$sapEncapValue$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProt Policy$*.
Cause	The sapDcpLocMonExcdAllDynFreed notification is generated for a particular SAP when all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLocMonPlcrLogEvent is configured to 'verbose'.
Effect	The affected SAP may be using more resources than expected and cause the system to under-perform.

Property name	Value
Recovery	There is no recovery required for this notification.

66.35 sapDcpLocMonExcdDynResource

Table 1119: sapDcpLocMonExcdDynResource properties

Property name	Value
Application name	SECURITY
Event ID	2061
Event name	sapDcpLocMonExcdDynResource
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.48
Default severity	warning
Message format string	Local monitor *$sapDcpFpLocMonPlcrName$* for sap *$sapEncap Value$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* detected as non-conformant at *$sapDcpTimeEventOccured$* and cannot allocate dynamic policers. Policy *$sapDCpuProtPolicy$*. Excd count=*$sapDcp FpLocMonExcdCount$*
Cause	The sapDcpLocMonExcdDynResource notification is generated when the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcements policers associated with the distributed CPU protection policy . This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLocMonPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected SAP may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP or to the dynamic enforcement policer pool(TIMETRA-CHASSIS-MIB.mib::tmnxFPDCpuProtDynEnfrcPlcr Pool).

66.36 sapDcpStaticConform

Table 1120: sapDcpStaticConform properties

Property name	Value
Application name	SECURITY
Event ID	2058
Event name	sapDcpStaticConform
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.45
Default severity	warning
Message format string	Sap *$sapEncapValue$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* newly conformant at *$sapDcpTimeEventOccured$*. Policy *$sapDCpu ProtPolicy$*. Policer=*$sapDcpFpStaticPlcrName$*(static). Excd count= *$sapDcpFpStaticExcdCount$*
Cause	The sapDcpStaticConform notification is generated when the static-policer for a particular SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected SAP is now in conformance with the parameters configured for the associated distributed CPU protection policy.
Recovery	There is no recovery required for this notification.

66.37 sapDcpStaticExcd

Table 1121: sapDcpStaticExcd properties

Property name	Value
Application name	SECURITY
Event ID	2052
Event name	sapDcpStaticExcd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.39
Default severity	warning
Message format string	Non conformant sap *$sapEncapValue$* on fp *$tmnxCardSlotNum $*/*$tmnxFPNum$* detected at *$sapDcpTimeEventOccured$*. Policy

Property name	Value
	$sapDCpuProtPolicy$. Policer= *$sapDcpFpStaticPlcrName$*(static). Excd count=*$sapDcpFpStaticExcdCount$*
Cause	The sapDcpStaticExcd notification is generated when the static-policer on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected SAP may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.

66.38 sapDcpStaticHoldDownEnd

Table 1122: sapDcpStaticHoldDownEnd properties

Property name	Value
Application name	SECURITY
Event ID	2056
Event name	sapDcpStaticHoldDownEnd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.43
Default severity	warning
Message format string	Hold-down completed for sap *$sapEncapValue$* on fp *$tmnxCard SlotNum$*/*$tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProtPolicy$*. Policer= *$sapDcpFpStaticPlcrName$*(static). Excd count=*$sapDcpFpStaticExcdCount$*
Cause	The sapDcpStaticHoldDownEnd notification is generated when a particular SAP completes hold-down period for an exceeding static-policer. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'verbose'.
Effect	The static-policer for an affected SAP will transition to a detection-time countdown after the hold-down period is complete.
Recovery	There is no recovery required for this notification.

66.39 sapDcpStaticHoldDownStart

Table 1123: sapDcpStaticHoldDownStart properties

Property name	Value
Application name	SECURITY
Event ID	2054
Event name	sapDcpStaticHoldDownStart
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.41
Default severity	warning
Message format string	Hold-down started for sap *$sapEncapValue$* on fp *$tmnxCardSlotNum $/$tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpu ProtPolicy$*. Policer= *$sapDcpFpStaticPlcrName$*(static). Excd count= *$sapDcpFpStaticExcdCount$*
Cause	The sapDcpStaticHoldDownStart notification is generated when a particular SAP starts hold-down period for an exceeding static-policer. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'verbose'.
Effect	The static-policer will treat all packets as non-conformant during the hold-down period.
Recovery	There is no recovery required for this notification.

66.40 SSH_server_preserve_key_fail

Table 1124: SSH_server_preserve_key_fail properties

Property name	Value
Application name	SECURITY
Event ID	2024
Event name	SSH_server_preserve_key_fail
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.1
Default severity	minor
Message format string	Persistance of SSH server host key failed on *$tmnxCpmFlashHwIndex $* with operational status *$tmnxCpmFlashOperStatus$*.
Cause	Persistance of the SSH server host keys failed.

Property name	Value
Effect	The SSH server host key will differ after reboot. The remote server host key will not be stored across reboots.
Recovery	N/A

66.41 ssh_user_login

Table 1125: ssh_user_login properties

Property name	Value
Application name	SECURITY
Event ID	2009
Event name	ssh_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged in
Cause	A user was successfully authenticated for login.
Effect	The user access session was started.
Recovery	No recovery is required

66.42 ssh_user_login_failed

Table 1126: ssh_user_login_failed properties

Property name	Value
Application name	SECURITY
Event ID	2011
Event name	ssh_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* failed authentication

Property name	Value
Cause	A user failed authentication.
Effect	The user access session was not started. The user will be given another opportunity to authenticate himself.
Recovery	No recovery is required

66.43 ssh_user_login_max_attempts

Table 1127: ssh_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2012
Event name	ssh_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.48
Default severity	minor
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A tmnxUserSshLoginMaxAttempts notification is generated when a user attempting to connect via SSH failed to authenticate for more than a maximum allowed number of times in a period of tmnxPassword AttemptsTime minutes. The value of the object tmnxPasswordAttempts Count indicates the maximum number of unsuccessful login attempts allowed. The value of the object tmnxPasswordAttemptsLockoutPeriod indicates the number of minutes the user is locked out if the threshold of unsuccessful login attempts has been exceeded. The value of the object tmnxSecNotifyUserName indicates the name of the user attempting to connect via SSH. The value of the object tmnxSecNotify AddrType indicates the type of the IP address stored in the object tmnx SecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to connect via SSH.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. An SSH session is terminated.
Recovery	No recovery action is required.

66.44 ssh_user_logout

Table 1128: ssh_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2010
Event name	ssh_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

66.45 sysDNSSecFailedAuthentication

Table 1129: sysDNSSecFailedAuthentication properties

Property name	Value
Application name	SECURITY
Event ID	2086
Event name	sysDNSSecFailedAuthentication
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.57
Default severity	warning
Message format string	Possible messages: • Received response for '*$tmnxSysDNSSecDomainName$*' from DNS Security aware server, the AD-bit is not set, response accepted • Received response for '*$tmnxSysDNSSecDomainName$*' from DNS Security aware server, the AD-bit is not set, response dropped
Cause	The sysDNSSecFailedAuthentication notification is generated when a DNS response PDU is received with an unset AD-bit and sysDNSSec AdValidation is set to 'true (1)'.

Property name	Value
Effect	This notification is informational only. The message will vary depending on the state of sysDNSSecRespCtrl.
Recovery	There is no recovery required for this notification.

66.46 tacplusInetSrvrOperStatusChange

Table 1130: tacplusInetSrvrOperStatusChange properties

Property name	Value
Application name	SECURITY
Event ID	2025
Event name	tacplusInetSrvrOperStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.35
Default severity	minor
Message format string	TACACS+ server *$tacPlusServerInetAddress$* operational status changed to *$tacplusServerOperStatus$*.
Cause	The operational status of a TACACS+ server has transitioned either from 'up' to 'down' or from 'down' to 'up'.
Effect	N/A
Recovery	No recovery is necessary.

66.47 tacplusOperStatusChange

Table 1131: tacplusOperStatusChange properties

Property name	Value
Application name	SECURITY
Event ID	2018
Event name	tacplusOperStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.20
Default severity	minor

Property name	Value
Message format string	TACACS+ operational status changed to *$tacplusOperStatus$*.
Cause	The TACACS+ operational status has transitioned either from 'up' to 'down' or from 'down' to 'up'.
Effect	N/A
Recovery	No recovery is necessary.

66.48 tmnxAppPkiCertVerificationFailed

Table 1132: tmnxAppPkiCertVerificationFailed properties

Property name	Value
Application name	SECURITY
Event ID	2116
Event name	tmnxAppPkiCertVerificationFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.51
Default severity	minor
Message format string	*$tmnxSecNotifClientAppName$* : Certificate *$tmnxSecNotifCert$* verification failed due to *$tmnxSecNotifFailureReason$*
Cause	The tmnxAppPkiCertVerificationFailed notification is generated when an attempt to verify the certificate fails for a non-IPsec application.
Effect	Fail to establish a secured connection with the remote entity.
Recovery	Make sure the certificate specified in tmnxSecNotifCert is a valid certificate and an appropriate trust anchor is configured.

66.49 tmnxCAProfileStateChange

Table 1133: tmnxCAProfileStateChange properties

Property name	Value
Application name	SECURITY
Event ID	2045
Event name	tmnxCAProfileStateChange

Property name	Value
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.18
Default severity	minor
Message format string	CA profile *$tmnxPkiCAProfile$* changed state to *$tmnxPkiCAProfile OperState$ $tmnxSecNotifFailureReason$*
Cause	The tmnxCAProfileStateChange notification is generated when Certificate Authority profile changes state to 'down' due to tmnxSecNotif FailureReason.
Effect	Certificate Authority profile will remain in this state until a corrective action is taken.
Recovery	Depending on the reason indicated by tmnxSecNotifFailureReason, corrective action should be taken.

66.50 tmnxCAProfUpDueToRevokeChkCrlOpt

Table 1134: tmnxCAProfUpDueToRevokeChkCrlOpt properties

Property name	Value
Application name	SECURITY
Event ID	2094
Event name	tmnxCAProfUpDueToRevokeChkCrlOpt
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.27
Default severity	minor
Message format string	CA profile *$tmnxPkiCAProfile$* changed state to *$tmnxPkiCAProfile OperState$* regardless of *$tmnxSecNotifFailureReason$* due to crl-optional is set
Cause	The tmnxCAProfUpDueToRevokeChkCrlOpt notification is generated when Certificate Authority profile changes state to 'up' due to tmnx PkiCAProfRevokeChk set to 'crlOptional' even with the errors in tmnx SecNotifFailureReason.
Effect	Certificate Authority profile will remain up.
Recovery	Errors described in tmnxSecNotifFailureReason should still be corrected.

66.51 tmnxCertExport

Table 1135: tmnxCertExport properties

Property name	Value
Application name	SECURITY
Event ID	2233
Event name	tmnxCertExport
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.58
Default severity	minor
Message format string	admin certificate export type *$tmnxSecNotifyImportExportType$* input *$tmnxSecNotifyUrl$* output *$tmnxSecNotifFile$* format *$tmnxSecNotifyImportExportFormat$* : *$tmnxSecEventOutcome$*
Cause	A tmnxCertExport notification is generated when a user exports a cryptographic key, certificate, or CRL with the admin certificate command
Effect	N/A
Recovery	N/A

66.52 tmnxCertImport

Table 1136: tmnxCertImport properties

Property name	Value
Application name	SECURITY
Event ID	2232
Event name	tmnxCertImport
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.57
Default severity	minor
Message format string	admin certificate import *$tmnxSecNotifyImportExportType$* input *$tmnxSecNotifyUrl$* output *$tmnxSecNotifFile$* format *$tmnxSecNotifyImportExportFormat$* : *$tmnxSecEventOutcome$*
Cause	A tmnxCertImport notification is generated when a user imports a cryptographic key, certificate, or CRL with the admin certificate command

Property name	Value
Effect	N/A
Recovery	N/A

66.53 tmnxCertKeyPairGen

Table 1137: tmnxCertKeyPairGen properties

Property name	Value
Application name	SECURITY
Event ID	2231
Event name	tmnxCertKeyPairGen
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.56
Default severity	minor
Message format string	Possible messages: • admin certificate gen-keypair *$tmnxSecNotifyUrl$* curve *$tmnxSecNotifyCurve$* : *$tmnxSecEventOutcome$* • admin certificate gen-keypair *$tmnxSecNotifyUrl$* size *$tmnxSecNotifyKeySize$* type *$tmnxSecNotifyKeyType$* : *$tmnxSecEventOutcome$*
Cause	A tmnxCertKeyPairGen notification is generated when a user generates a cryptographic key with the admin certificate command
Effect	N/A
Recovery	N/A

66.54 tmnxCliGroupSessionLimitExceeded

Table 1138: tmnxCliGroupSessionLimitExceeded properties

Property name	Value
Application name	SECURITY
Event ID	2112
Event name	tmnxCliGroupSessionLimitExceeded

Property name	Value
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.44
Default severity	minor
Message format string	*$tmnxSessionLimitExceededType$* of CLI session group ' *$tmnx SessionLimitExceededName$*' has been exceeded
Cause	The tmnxCliGroupSessionLimitExceeded notification is generated when an attempt to establish a new user access session is not successful because any of SSH / Telnet / Total session limits defined for the CLI session group of which the user is an indirect member (as a member of a user profile that is a member of the CLI session group) has been exceeded. The value of the object tmnxSessionLimit ExceededName indicates the name of the CLI session group of which the session limit has been exceeded. The value of the object tmnx SessionLimitExceededType indicates the type of the session limit that has been exceeded.
Effect	The user access session has not been established.
Recovery	An administrator may execute one of the following actions in order to allow a successful session establishment: 1) force disconnection of an existing session(s) using 'admin disconnect' CLI command 2) increase the value of the session limit using CLI or SNMP SET operation on the corresponding object in tmnxCliSessionGroupTable 3) revoke the profile membership for the particular user (beware that this action may have impact on user's priviledges) 4) revoke the session group membership for the particular profile

66.55 tmnxConfigCreate

Table 1139: tmnxConfigCreate properties

Property name	Value
Application name	SECURITY
Event ID	2207
Event name	tmnxConfigCreate
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* managed object created

Property name	Value
Cause	A new row entry was created in one of the MIB tables. This event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

66.56 tmnxConfigDelete

Table 1140: tmnxConfigDelete properties

Property name	Value
Application name	SECURITY
Event ID	2208
Event name	tmnxConfigDelete
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.10
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* managed object deleted
Cause	An existing row entry in one of the MIB tables is deleted. This event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

66.57 tmnxConfigModify

Table 1141: tmnxConfigModify properties

Property name	Value
Application name	SECURITY
Event ID	2206
Event name	tmnxConfigModify
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.8

Property name	Value
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* configuration modified
Cause	A configuration attribute associated with a row entry in a MIB table was modified. this event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

66.58 tmnxCpmProtDefPolModified

Table 1142: tmnxCpmProtDefPolModified properties

Property name	Value
Application name	SECURITY
Event ID	2037
Event name	tmnxCpmProtDefPolModified
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.11
Default severity	minor
Message format string	Default policy *$tmnxCpmProtPolId$* being modified by user.
Cause	User modifies default access or default network policy.
Effect	N/A
Recovery	No recovery is necessary.

66.59 tmnxCpmProtExcdSapEcm

Table 1143: tmnxCpmProtExcdSapEcm properties

Property name	Value
Application name	SECURITY
Event ID	2041
Event name	tmnxCpmProtExcdSapEcm

Property name	Value
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.14
Default severity	warning
Message format string	Eth-CFM packet arrival rate exceeded for Eth-CFM opcode *$tmnxCpmProtExcdSapEcmOpCode$* domain level *$tmnxCpmProtExcdSapEcmLevel$* MAC *$tmnxCpmProtExcdSapEcmMac$* SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	The tmnxCpmProtExcdSapEcm notification is generated when an Eth-CFM packet stream (identified by a source MAC address, domain level, and Eth-CFM opcode) arrives at a local SAP at a rate which exceeds the configured Eth-CFM rate limit for the stream.
Effect	One or more Eth-CFM packets arriving at the SAP was discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the locally configured Eth-CFM rate limit for the stream.

66.60 tmnxCpmProtExcdSapIp

Table 1144: tmnxCpmProtExcdSapIp properties

Property name	Value
Application name	SECURITY
Event ID	2046
Event name	tmnxCpmProtExcdSapIp
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.19
Default severity	warning
Message format string	Per-source packet arrival rate exceeded for IP *$tmnxCpmProtExcdSapIpAddr$* SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	The tmnxCpmProtExcdSapIp notification is generated when a source (identified by an IP address) sends a packet stream to a local SAP at a rate which exceeds the SAP's configured per-source-rate. [EFFECT] One or more packets arriving at the SAP was discarded. [RECOVERY] Reduce the packet transmission rate at the far end, OR increase the locally configured per-source-rate for the SAP, OR disable per-IP-source rate limiting on the SAP by setting TIMETRA-SAP-MIB::sapCpmProtMonitorIP to 'false'.

Property name	Value
Effect	N/A
Recovery	N/A

66.61 tmnxCpmProtExcdSdpBind

Table 1145: tmnxCpmProtExcdSdpBind properties

Property name	Value
Application name	SECURITY
Event ID	2040
Event name	tmnxCpmProtExcdSdpBind
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.13
Default severity	warning
Message format string	Per-source packet arrival rate exceeded for MAC *$tmnxCpmProtExcdSdpBindMac$* SDP Bind *$sdpBindId$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	The tmnxCpmProtExcdSdpBind notification is generated when a source (identified by a MAC address) sends a packet stream to a local mesh-sdp or spoke-sdp at a rate which exceeds the SDP's configured per-source-rate.
Effect	One or more packets arriving at the mesh-sdp or spoke-sdp was discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the locally configured per-source-rate for the SDP.

66.62 tmnxCpmProtExcdSdpBindEcm

Table 1146: tmnxCpmProtExcdSdpBindEcm properties

Property name	Value
Application name	SECURITY
Event ID	2042
Event name	tmnxCpmProtExcdSdpBindEcm

Property name	Value
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.15
Default severity	warning
Message format string	Eth-CFM packet arrival rate exceeded for Eth-CFM opcode *$tmnxCpmProtExcdSdpBindEcmOpCode$* domain level *$tmnxCpmProtExcdSdpBindEcmLevel$* MAC *$tmnxCpmProtExcdSdpBindEcmMac$* SDP Bind *$sdpBindId$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	The tmnxCpmProtExcdSdpBindEcm notification is generated when an Eth-CFM packet stream (identified by a source MAC address, domain level, and Eth-CFM opcode) arrives at a local mesh-sdp or spoke-sdp at a rate which exceeds the configured Eth-CFM rate limit for the stream.
Effect	One or more Eth-CFM packets arriving at the mesh-sdp or spoke-sdp was discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the locally configured Eth-CFM rate limit for the stream.

66.63 tmnxCpmProtExcdSdpBindIp

Table 1147: tmnxCpmProtExcdSdpBindIp properties

Property name	Value
Application name	SECURITY
Event ID	2087
Event name	tmnxCpmProtExcdSdpBindIp
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.23
Default severity	warning
Message format string	Per-source packet arrival rate exceeded for IP *$tmnxCpmProtExcdSdpBindIpAddr$* SDP Bind *$sdpBindId$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	The tmnxCpmProtExcdSdpBindIp notification is generated when a source (identified by an IP address) sends a packet stream to a local mesh-sdp or spoke-sdp at a rate which exceeds the SDP's configured per-source-rate.
Effect	One or more packets arriving at the mesh-sdp or spoke-sdp was discarded.

Property name	Value
Recovery	Reduce the packet transmission rate at the far end, or increase the locally configured per-source-rate for the SDP.

66.64 tmnxCpmProtViolIf

Table 1148: tmnxCpmProtViolIf properties

Property name	Value
Application name	SECURITY
Event ID	2030
Event name	tmnxCpmProtViolIf
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.5
Default severity	warning
Message format string	Overall packet arrival rate exceeded for interface *$vRtrIfIndex$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	A overall packet arrival rate limit violation was detected for an interface and notifications are enabled. The overall packet arrival rate limit is specified by the managed object tmnxCpmProtPolOverallRateLimit of the interface protection policy specified by the managed object TIMETRA-VRTR-MIB::vRtrIfCpmProtPolicyId. Notifications are enabled if the value of the managed object tmnxCpmProtPolAlarm of the interface protection policy specified by the managed object TIMETRA-VRTR-MIB::vRtrIfCpmProtPolicyId is equal to 'true'. The notification may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the managed object tmnxCpmProtPolOverallRateLimit. Additional information can be retrieved in the SNMP table tmnxCpm ProtViolIfTable.
Effect	While the overall packet arrival rate limit is being exceeded, some protocol packets are dropped.
Recovery	No recovery is necessary.

66.65 tmnxCpmProtViolIfOutProf

Table 1149: tmnxCpmProtViolIfOutProf properties

Property name	Value
Application name	SECURITY
Event ID	2085
Event name	tmnxCpmProtViolIfOutProf
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.22
Default severity	warning
Message format string	Out-of-Profile control packets rate exceeded for interface *$vRtrIfIndex$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	The tmnxCpmProtViolIfOutProf notification is generated when the rate at which incoming control packets are marked as out-of-profile specified by tmnxCpmProtPolOutProfileRate is exceeded. This notification is generated when tmnxCpmProtPolOutProfRateLogEvnt is set to 'true'.
Effect	One or more control packets being marked as out-of-profile will be discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the out-of-profile rate, tmnxCpmProtPolOutProfileRate for this interface.

66.66 tmnxCpmProtViolMac

Table 1150: tmnxCpmProtViolMac properties

Property name	Value
Application name	SECURITY
Event ID	2032
Event name	tmnxCpmProtViolMac
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.7
Default severity	warning
Message format string	Per-source packet arrival rate exceeded for MAC *$tmnxCpmProtViolMacAddress$* SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*

Property name	Value
Cause	A per-source rate limit violation was detected for a source, and notifications are enabled. The per-source rate limit is specified by the object tmnxCpmProtPolPerSrcRateLimit of the SAP protection policy specified by the object TIMETRA-SAP-MIB::sapCpmProtPolicyId. Notifications are enabled if the value of the object tmnxCpmProtPol Alarm of the SAP protection policy specified by the object TIMETRA-SAP-MIB::sapCpmProtPolicyId is equal to 'true'. The notification may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the tmnxCpmProtPolPerSrcRateLimit Additional information can be retrieved in the table tmnxCpmProtExcdTable.
Effect	While the per-source rate limit is being exceeded, some protocol packets are dropped.
Recovery	No recovery is necessary.

66.67 tmnxCpmProtViolPort

Table 1151: tmnxCpmProtViolPort properties

Property name	Value
Application name	SECURITY
Event ID	2028
Event name	tmnxCpmProtViolPort
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.3
Default severity	warning
Message format string	Link-specific packet arrival rate limit exceeded for port *$tmnxPortPortID $*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	A link-specific packet arrival rate limit violation was detected for a port. The link-specific packet arrival rate limit is specified by the managed object tmnxCpmProtLinkRateLimit. This event may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the managed object tmnxCpmProtLinkRateLimit. Additional information can be retrieved from the SNMP table tmnxCpmProtViolPortTable.
Effect	While the link-specific packet arrival rate limit is being exceeded, some packets from link-specific protocols are dropped.
Recovery	No recovery is necessary.

66.68 tmnxCpmProtViolPortAgg

Table 1152: tmnxCpmProtViolPortAgg properties

Property name	Value
Application name	SECURITY
Event ID	2029
Event name	tmnxCpmProtViolPortAgg
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.4
Default severity	warning
Message format string	Per-port overall packet rate limit exceeded for port *$tmnxPortPortID$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	A per-port overall packet rate limit violation was detected for a port. The per-port overall packet rate limit is specified by the managed object tmnxCpmProtPortOverallRateLimit. This event may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the managed object tmnxCpmProtPortOverallRateLimit. Additional information can be retrieved from the SNMP table tmnxCpmProtViol PortTable.
Effect	While the link-specific packet arrival rate limit is being exceeded, some protocol packets are dropped.
Recovery	No recovery is necessary.

66.69 tmnxCpmProtViolSap

Table 1153: tmnxCpmProtViolSap properties

Property name	Value
Application name	SECURITY
Event ID	2031
Event name	tmnxCpmProtViolSap
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.6
Default severity	warning
Message format string	Overall packet arrival rate exceeded for SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPkt HexDump$*

Property name	Value
Cause	A overall packet arrival rate limit violation was detected for a SAP and notifications are enabled. The overall packet arrival rate limit is specified by the object tmnxCpmProtPolOverallRateLimit of the SAP protection policy specified by the object TIMETRA-SAP-MIB::sap CpmProtPolicyId. Notifications are enabled if the value of the object tmnxCpmProtPolAlarm of the SAP protection policy specified by the object TIMETRA-SAP-MIB::sapCpmProtPolicyId is equal to 'true'. The notification may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the tmnxCpmProtPolOverallRateLimit Additional information can be retrieved in the table tmnxCpmProtViol SapTable.
Effect	While the overall packet arrival rate limit is being exceeded, some protocol packets are dropped.
Recovery	No recovery is necessary.

66.70 tmnxCpmProtViolSapOutProf

Table 1154: tmnxCpmProtViolSapOutProf properties

Property name	Value
Application name	SECURITY
Event ID	2084
Event name	tmnxCpmProtViolSapOutProf
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.21
Default severity	warning
Message format string	Out-of-Profile control packets rate exceeded for SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcd PktHexDump$*
Cause	The tmnxCpmProtViolSapOutProf notification is generated when the rate at which incoming control packets are marked as out-of-profile specified by tmnxCpmProtPolOutProfileRate is exceeded. This notification is generated when tmnxCpmProtPolOutProfRateLogEvnt is set to 'true'.
Effect	One or more control packets being marked as out-of-profile will be discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the out-of-profile rate, tmnxCpmProtPolOutProfileRate for this SAP.

66.71 tmnxCpmProtViolSdpBind

Table 1155: tmnxCpmProtViolSdpBind properties

Property name	Value
Application name	SECURITY
Event ID	2039
Event name	tmnxCpmProtViolSdpBind
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.12
Default severity	warning
Message format string	Overall packet arrival rate exceeded for SDP Bind *$sdpBindId$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPkt HexDump$*
Cause	The tmnxCpmProtViolSdpBind notification is generated when the packet arrival rate at a mesh-sdp or spoke-sdp exceeds the SDP's configured overall-rate.
Effect	One or more packets arriving at the mesh-sdp or spoke-sdp was discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the locally configured overall-rate for the SDP.

66.72 tmnxCpmProtViolSdpBindOutProf

Table 1156: tmnxCpmProtViolSdpBindOutProf properties

Property name	Value
Application name	SECURITY
Event ID	2089
Event name	tmnxCpmProtViolSdpBindOutProf
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.25
Default severity	warning
Message format string	Out-of-Profile control packets rate exceeded for SDP Bind *$sdpBindId$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcd PktHexDump$*

Property name	Value
Cause	The tmnxCpmProtViolSdpBindOutProf notification is generated when the rate at which incoming control packets are marked as out-of-profile specified by tmnxCpmProtPolOutProfileRate is exceeded. This notification is generated when tmnxCpmProtPolOutProfRateLogEvnt is set to 'true'.
Effect	One or more control packets being marked as out-of-profile will be discarded.
Recovery	Reduce the packet transmission rate at the far end, or increase the out-of-profile rate, tmnxCpmProtPolOutProfileRate for this SDP binding.

66.73 tmnxCpmProtViolVdoSvcClient

Table 1157: tmnxCpmProtViolVdoSvcClient properties

Property name	Value
Application name	SECURITY
Event ID	2033
Event name	tmnxCpmProtViolVdoSvcClient
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.8
Default severity	warning
Message format string	Per-source rate limit exceeded for source *$tmnxCpmProtViolVdoSvcCltAddr$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	N/A
Effect	N/A
Recovery	N/A

66.74 tmnxCpmProtViolVdoVrtrClient

Table 1158: tmnxCpmProtViolVdoVrtrClient properties

Property name	Value
Application name	SECURITY
Event ID	2034

Property name	Value
Event name	tmnxCpmProtViolVdoVrtrClient
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.9
Default severity	warning
Message format string	Per-source rate limit exceeded for source *$tmnxCpmProtViolVdoVrtrCltAddr$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
Cause	N/A
Effect	N/A
Recovery	N/A

66.75 tmnxDcpCardFpEventOvrflw

Table 1159: tmnxDcpCardFpEventOvrflw properties

Property name	Value
Application name	SECURITY
Event ID	2080
Event name	tmnxDcpCardFpEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.72
Default severity	warning
Message format string	Distributed CPU Protection FP log event overflow occured on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpCardFpEventOvrflw notification is generated when a flood of distibuted CPU protection events occur on a particular card and some of the events are lost due to event throttling mechanism.
Effect	Some notifications configured on the card may not be received.
Recovery	Notifications will resume once the event throttling ends.

66.76 tmnxDcpCardFpEventOvrflwClr

Table 1160: tmnxDcpCardFpEventOvrflwClr properties

Property name	Value
Application name	SECURITY
Event ID	2049
Event name	tmnxDcpCardFpEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.77
Default severity	warning
Message format string	*$tmnxDcpMissingNotificationCount$* Distributed CPU Protection FP log events were dropped in the last event throttling interval on card *$tmnx ChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpCardFpEventOvrflwClr notification is generated when the event throttling has ended for distibuted CPU protection FP events on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

66.77 tmnxDcpCardSapEventOvrflw

Table 1161: tmnxDcpCardSapEventOvrflw properties

Property name	Value
Application name	SECURITY
Event ID	2081
Event name	tmnxDcpCardSapEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.73
Default severity	warning
Message format string	Distributed CPU Protection SAP log event overflow occured on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpCardSapEventOvrflw notification is generated when a flood of distibuted CPU protection SAP events occur on a particular card and some of the events are lost due to event throttling mechanism.

Property name	Value
Effect	Some SAP notifications configured on the card may not be received.
Recovery	Notifications will resume once the event throttling ends.

66.78 tmnxDcpCardSapEventOvrflwClr

Table 1162: tmnxDcpCardSapEventOvrflwClr properties

Property name	Value
Application name	SECURITY
Event ID	2050
Event name	tmnxDcpCardSapEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.78
Default severity	warning
Message format string	*$tmnxDcpMissingNotificationCount$* Distributed CPU Protection SAP log events were dropped in the last event throttling interval on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpCardSapEventOvrflwClr notification is generated when the event throttling has ended for distibuted CPU protection SAP events on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

66.79 tmnxDcpCardVrtrIfEventOvrflw

Table 1163: tmnxDcpCardVrtrIfEventOvrflw properties

Property name	Value
Application name	SECURITY
Event ID	2082
Event name	tmnxDcpCardVrtrIfEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.74
Default severity	warning

Property name	Value
Message format string	Distributed CPU Protection Network_if log event overflow occured on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEvent Occured$*
Cause	The tmnxDcpCardVrtrIfEventOvrflw notification is generated when a flood of distibuted CPU protection network-interface events occur on a particular card and some of the events are lost due to event throttling mechanism.
Effect	Some network-interface notifications configured on the card may not be received.
Recovery	Notifications will resume once the event throttling ends.

66.80 tmnxDcpCardVrtrIfEventOvrflwClr

Table 1164: tmnxDcpCardVrtrIfEventOvrflwClr properties

Property name	Value
Application name	SECURITY
Event ID	2051
Event name	tmnxDcpCardVrtrIfEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.79
Default severity	warning
Message format string	*$tmnxDcpMissingNotificationCount$* Distributed CPU Protection Netwk_if log events were dropped in the last event throttling interval on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEvent Occured$*
Cause	The tmnxDcpCardVrtrIfEventOvrflwClr notification is generated the when event throttling has ended for distibuted CPU protection networrk-interface events on a particular card.
Effect	Notifications are received again since the event throttling has ended.
Recovery	There is no recovery for this notification.

66.81 tmnxDcpFpDynPoolUsageHiAlmClear

Table 1165: tmnxDcpFpDynPoolUsageHiAlmClear properties

Property name	Value
Application name	SECURITY
Event ID	2048
Event name	tmnxDcpFpDynPoolUsageHiAlmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.76
Default severity	warning
Message format string	Dynamic Enforcement Pool OK again on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpFpDynPoolUsageHiAlmClear notification is generated when the dynamic enforcement policer pool usage on the forwarding plane is no longer exhausted.
Effect	Dynamic enforcement policers are available in the free pool to be allocated when needed.
Recovery	There is no recovery required for this notification.

66.82 tmnxDcpFpDynPoolUsageHiAlmRaise

Table 1166: tmnxDcpFpDynPoolUsageHiAlmRaise properties

Property name	Value
Application name	SECURITY
Event ID	2047
Event name	tmnxDcpFpDynPoolUsageHiAlmRaise
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.75
Default severity	warning
Message format string	Dynamic Enforcement Pool nearly (or fully) exhausted on fp *$tmnxCard SlotNum$*/*$tmnxFPNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpFpDynPoolUsageHiAlmRaise notification is generated when the dynamic enforcement policer pool usage on the forwarding plane is nearly exhausted.

Property name	Value
Effect	Dynamic enforcement policers may not get allocated on the forwarding plane.
Recovery	This notification will be cleared when either the dynamic enforcement policer pool is increased or the usage drops.

66.83 tmnxFileCopied

Table 1167: tmnxFileCopied properties

Property name	Value
Application name	SECURITY
Event ID	2236
Event name	tmnxFileCopied
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.61
Default severity	minor
Message format string	File *$tmnxSecNotifyUrl$* copied to *$tmnxSecNotifyNewUrl$* : *$tmnxSecEventOutcome$*
Cause	A tmnxFileCopied notification is generated when a user copies a file through the file command
Effect	N/A
Recovery	N/A

66.84 tmnxFileDeleted

Table 1168: tmnxFileDeleted properties

Property name	Value
Application name	SECURITY
Event ID	2234
Event name	tmnxFileDeleted
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.59
Default severity	minor

Property name	Value
Message format string	File *$tmnxSecNotifyUrl$* delete : *$tmnxSecEventOutcome$*
Cause	A tmnxFileDeleted notification is generated when a user deletes a file through the file command
Effect	N/A
Recovery	N/A

66.85 tmnxFileMoved

Table 1169: tmnxFileMoved properties

Property name	Value
Application name	SECURITY
Event ID	2235
Event name	tmnxFileMoved
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.60
Default severity	minor
Message format string	File *$tmnxSecNotifyUrl$* move to *$tmnxSecNotifyNewUrl$* : *$tmnxSec EventOutcome$*
Cause	A tmnxFileMoved notification is generated when a user moves a file through the file command
Effect	N/A
Recovery	N/A

66.86 tmnxKeyChainAuthFailure

Table 1170: tmnxKeyChainAuthFailure properties

Property name	Value
Application name	SECURITY
Event ID	2027
Event name	tmnxKeyChainAuthFailure

Property name	Value
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.2
Default severity	minor
Message format string	Incoming packet from source address *$tmnxKeyChainAuthAddress$* virtual router *$vRtrID$* dropped due to key chain authentication failure and possible reason is *$tmnxKeyChainAuthFailReason$*.
Cause	The incoming packet was dropped due to key chain authentication failure. Failure could be due to the following reasons or more: - Send packet had no auth keychain but recv side had keychain enabled. - Keychain key id's did not match. - Keychain key digest mismatch. - Received packet with and invalid enhanced authentication option length. - For other causes of failure refer to 'draft-bonica-tcp-auth-05.txt'.
Effect	N/A
Recovery	No recovery is necessary.

66.87 tmnxMD5AuthFailure

Table 1171: tmnxMD5AuthFailure properties

Property name	Value
Application name	SECURITY
Event ID	2036
Event name	tmnxMD5AuthFailure
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.10
Default severity	minor
Message format string	Incoming packet from source address *$tmnxMD5AuthAddr$* virtual router *$vRtrID$* dropped due to MD5 authentication failure and possible reason is *$tmnxMD5AuthFailReason$*.
Cause	The incoming packet was dropped due to MD5 authentication failure. Failure is due to digest mismatch.
Effect	N/A
Recovery	No recovery is necessary.

66.88 tmnxPasswordHashingChanged

Table 1172: tmnxPasswordHashingChanged properties

Property name	Value
Application name	SECURITY
Event ID	2238
Event name	tmnxPasswordHashingChanged
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.63
Default severity	minor
Message format string	Password hashing changed from *$tmnxSecNotifOldPasswordHashing$* to *$tmnxSecNotifNewPasswordHashing$*
Cause	The tmnxPasswordHashingChanged notification is generated upon the change of password hashing algorithm (tmnxPasswordHashing). The value of the object tmnxSecNotifNewPasswordHashing indicates the new password hashing algorithm. The value of the object tmnxSecNotif OldPasswordHashing indicates the new password hashing algorithm.
Effect	Users will be prompted to change their password upon log in to the system. All newly stored user passwords will be hashed by the algorithm defined by tmnxPasswordHashing.
Recovery	No recovery action is required.

66.89 tmnxPkiCAProfActnStatusChg

Table 1173: tmnxPkiCAProfActnStatusChg properties

Property name	Value
Application name	SECURITY
Event ID	2083
Event name	tmnxPkiCAProfActnStatusChg
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.20
Default severity	minor
Message format string	*$tmnxPkiCAProfActnType$* for ca-profile (*$tmnxPkiCAProfile$*) *$tmnx PkiCAProfActnStatus$*. ca-response: *$tmnxCAProfActnStatusCode$*. *$tmnxPkiCAProfActnStatusString$*

Property name	Value
Cause	The tmnxPkiCAProfActnStatusChg notification is generated when tmnx PkiCAProfActnStatus changes status. More information is available through tmnxPkiCAProfActnStatusString and tmnxPkiCAProfActn StatusCode.
Effect	This is due to the action performed using tmnxPkiCAProfActnTable.
Recovery	Depending on the information available in this trap, another tmnx PkiCAProfActnType request may be issued by correcting the parameters in the tmnxPkiCAProfActnTable.

66.90 tmnxPkiCAProfCrlUpdAllUrlsFail

Table 1174: tmnxPkiCAProfCrlUpdAllUrlsFail properties

Property name	Value
Application name	SECURITY
Event ID	2108
Event name	tmnxPkiCAProfCrlUpdAllUrlsFail
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.40
Default severity	minor
Message format string	Failed to update the CRL file from *$tmnxPkiCAProfUrl$* (*$tmnx PkiCAProfUrlId$*), the last of all the URLs for CA profile *$tmnx PkiCAProfile$*, due to *$tmnxSecNotifFailureReason$*
Cause	A tmnxPkiCAProfCrlUpdAllUrlsFail notification is generated when the CRL update operation failed after attempting all URLs for an existing CA Profile. The CA Profile is configured via tmnxPkiCAProfileTable. URLs for an existing CA Profile are configured via tmnxPkiCAProfUrl Table.
Effect	When tmnxPkiCAProfAtCrlUpdScheduleT is 'nextUpdateBased (1)' and tmnxPkiCAProfAtCrlUpdRetryIntv is zero, the system will stop attempting to update the CRL file. The system will attempt to download the same CRL file starting from the first URL in the URL list again after 1) tmnxPkiCAProfAtCrlUpdRetryIntv (>0) seconds, when tmnx PkiCAProfAtCrlUpdScheduleT is 'nextUpdateBased (1)', or 2) tmnx PkiCAProfAtCrlUpdPrdcUpdIntv seconds, when tmnxPkiCAProfAtCrl UpdScheduleT is 'periodic (2)'.
Recovery	Make sure the URLs specified in tmnxPkiCAProfUrlTable are correct.

66.91 tmnxPkiCAProfCrlUpdateStart

Table 1175: tmnxPkiCAProfCrlUpdateStart properties

Property name	Value
Application name	SECURITY
Event ID	2105
Event name	tmnxPkiCAProfCrlUpdateStart
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.37
Default severity	minor
Message format string	Started updating the CRL file for CA profile *$tmnxPkiCAProfileName ForNotify$*
Cause	A tmnxPkiCAProfCrlUpdateStart notification is generated when a CRL update operation is started for an existing CA Profile. The CA Profile is configured via tmnxPkiCAProfileTable.
Effect	The system is downloading the CRL file from a URL, which is configured via tmnxPkiCAProfUrlTable.
Recovery	No recovery is required for this notification.

66.92 tmnxPkiCAProfCrlUpdateSuccess

Table 1176: tmnxPkiCAProfCrlUpdateSuccess properties

Property name	Value
Application name	SECURITY
Event ID	2106
Event name	tmnxPkiCAProfCrlUpdateSuccess
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.38
Default severity	minor
Message format string	A CRL file was successfully updated from *$tmnxPkiCAProfUrl$* (*$tmnx PkiCAProfUrlId$*) for CA profile *$tmnxPkiCAProfile$*
Cause	A tmnxPkiCAProfCrlUpdateSuccess notification is generated when a new valid CRL file is successfully updated for an existing CA Profile. The CA Profile is configured via tmnxPkiCAProfileTable.

Property name	Value
Effect	tmnxPkiCAProfileCRLFile will be replaced if the downloaded CRL file qualified. The cases that a downloaded CRL does not qualify are explained in the description clause of tmnxPkiCAProfAtCrlUpd ScheduleT.
Recovery	No recovery is required for this notification.

66.93 tmnxPkiCAProfCrlUpdateUrlFail

Table 1177: tmnxPkiCAProfCrlUpdateUrlFail properties

Property name	Value
Application name	SECURITY
Event ID	2107
Event name	tmnxPkiCAProfCrlUpdateUrlFail
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.39
Default severity	minor
Message format string	Failed to update the CRL file from *$tmnxPkiCAProfUrl$* (*$tmnx PkiCAProfUrlId$*) due to *$tmnxSecNotifFailureReason$*
Cause	A tmnxPkiCAProfCrlUpdateUrlFail notification is generated when the CRL update operation has failed after attempting the indicated URL for an existing CA Profile. The CA Profile is configured via tmnx PkiCAProfileTable. URLs for an existing CA Profile are configured via tmnxPkiCAProfUrlTable. A tmnxPkiCAProfCrlUpdateUrlFail will not be sent when the URL is the last one in the URL list for an existing CA Profile. In such case, a tmnxPkiCAProfCrlUpdAllUrlsFail notification will be sent.
Effect	The system will attempt to download the CRL file from the next URL in the URL list.
Recovery	Make sure the URLs specified in tmnxPkiCAProfUrlTable are correct.

66.94 tmnxPkiCAProfCrlUpdLargPreUpdTm

Table 1178: tmnxPkiCAProfCrlUpdLargPreUpdTm properties

Property name	Value
Application name	SECURITY
Event ID	2113
Event name	tmnxPkiCAProfCrlUpdLargPreUpdTm
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.45
Default severity	minor
Message format string	The CRL pre-update time for CA profile *$tmnxPkiCAProfileNameFor Notify$* might be too large
Cause	A tmnxPkiCAProfCrlUpdLargPreUpdTm notification is generated when the 'nextUpdate' time of a newly downloaded CRL is earlier than the last successful update time or the time of setting tmnxPkiCAProfAtCrl UpdAdminState to 'inService (2)' plus the pre-update time. The last successful update time is stored in tmnxPkiCAProfAtCrlUpdLstSucs TmSt. The pre-update time is configured via tmnxPkiCAProfAtCrlUpd PreUpdTime.
Effect	The system will update the CRL again in tmnxPkiCAProfAtCrlUpdRetry Intv seconds rather than immediately.
Recovery	Configure tmnxPkiCAProfAtCrlUpdPreUpdTime to a value less than (the 'nextUpdate' value of the newly downloaded CRL - the last successful update time). The ideal value would be a value slightly lower than the CRL overlap period to avoid unnecessary download attempts. No recovery is needed for if the notification is generated in case of setting tmnxPkiCAProfAtCrlUpdAdminState to 'inService (2)'.

66.95 tmnxPkiCAProfCrlUpdNoNxtUpdTime

Table 1179: tmnxPkiCAProfCrlUpdNoNxtUpdTime properties

Property name	Value
Application name	SECURITY
Event ID	2110
Event name	tmnxPkiCAProfCrlUpdNoNxtUpdTime
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.42

Property name	Value
Default severity	minor
Message format string	No further scheduled CRL update for CA profile *$tmnxPkiCAProfile NameForNotify$* since either 1) the CRL update retry interval is not configured, or 2) 'nextUpdate' field is missing from the CRL, or 3) the 'nextUpdate' value is beyond the limit of the system
Cause	A tmnxPkiCAProfCrlUpdNoNxtUpdTime notification is generated when tmnxPkiCAProfAtCrlUpdScheduleT is 'nextUpdateBased (1)' and one of the following conditions is true: 1) The 'nextUpdate' field is missing from the CRL file or contains a value that is beyond the limit of the system 2) tmnxPkiCAProfAtCrlUpdRetryIntv is zero, and none of the configured URLs work or contain a CRL that qualifies from the first scheduled update.
Effect	The system will not download a new CRL file.
Recovery	Change tmnxPkiCAProfAtCrlUpdScheduleT to 'periodic (2)' if the system is to check for an updated CRL every tmnxPkiCAProfAtCrlUpd PrdcUpdIntv seconds. Otherwise, configure the tmnxPkiCAProfAtCrl UpdAdminState to 'outOfService (3)'.

66.96 tmnxPkiCAProfRevokeChkWarning

Table 1180: tmnxPkiCAProfRevokeChkWarning properties

Property name	Value
Application name	SECURITY
Event ID	2093
Event name	tmnxPkiCAProfRevokeChkWarning
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	*$tmnxSecNotifTunnelName$* : CRL check skipped for *$skippedCert$* issued by ca-profile *$tmnxPkiCAProfile$* while verifying EE cert *$ee CertSubject$* due to *$tmnxSecNotifFailureReason$*
Cause	The tmnxPkiCAProfRevokeChkWarning notification is generated whenever a CRL verification is skipped during chain/ee certificate verification. This event is throttled.
Effect	System did not verify revocation status on the subject certificate.

Property name	Value
Recovery	Check the value of tmnxPkiCAProfRevokeChk object for this CA profile if it is not expected.

66.97 tmnxPkiCertAfterExpWarning

Table 1181: tmnxPkiCertAfterExpWarning properties

Property name	Value
Application name	SECURITY
Event ID	2096
Event name	tmnxPkiCertAfterExpWarning
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.29
Default severity	minor
Message format string	Certificate *$tmnxSecNotifFile$* used by *$tmnxSecNotifClientAppName$* has expired.
Cause	The tmnxPkiCertAfterExpWarning notification is generated when the certificate indicated in tmnxSecNotifFile has expired.
Effect	The indicated certificate has expired.
Recovery	Replace the indicated file with an updated certificate.

66.98 tmnxPkiCertBeforeExpWarning

Table 1182: tmnxPkiCertBeforeExpWarning properties

Property name	Value
Application name	SECURITY
Event ID	2095
Event name	tmnxPkiCertBeforeExpWarning
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.28
Default severity	minor

Property name	Value
Message format string	Certificate *$tmnxSecNotifFile$* used by *$tmnxSecNotifClientAppName$* will expire in *$tmnxPkiExpRemainingHours$* hour(s) and *$tmnxPkiExpRemainingMinutes$* minute(s).
Cause	The tmnxPkiCertBeforeExpWarning notification is generated when the certificate indicated in tmnxSecNotifFile will expire in the time period indicated by tmnxPkiExpRemainingHours and tmnxPkiExpRemainingMinutes.
Effect	The indicated certificate will expire.
Recovery	Replace the indicated file with an updated certificate.

66.99 tmnxPkiCertExpWarningCleared

Table 1183: tmnxPkiCertExpWarningCleared properties

Property name	Value
Application name	SECURITY
Event ID	2097
Event name	tmnxPkiCertExpWarningCleared
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.30
Default severity	minor
Message format string	Expiration warning for certificate *$tmnxSecNotifFile$* used by *$tmnxSecNotifClientAppName$* is no longer applicable because of the following reason: *$tmnxPkiExpReason$*.
Cause	The tmnxPkiCertExpWarningCleared notification is generated when the expiration warning for the certificate indicated in tmnxSecNotifFile no longer applies because of the reason indicated in tmnxPkiExpReason.
Effect	The indicated certificate is no longer going to expire.
Recovery	None needed.

66.100 tmnxPkiCertNotYetValid

Table 1184: tmnxPkiCertNotYetValid properties

Property name	Value
Application name	SECURITY
Event ID	2114
Event name	tmnxPkiCertNotYetValid
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.49
Default severity	minor
Message format string	Certificate *$tmnxSecNotifFile$* used by *$tmnxSecNotifClientAppName$* is not yet valid.
Cause	The tmnxPkiCertNotYetValid notification is generated when the certificate indicated in tmnxSecNotifFile is not yet valid.
Effect	The indicated certificate is not usable until the 'notBefore' time is reached. If the certificate is specified in a CA-profile, then the operational state of the CA-profile (i.e., tmnxPkiCAProfileOperState) remains down until the 'notBefore' time is reached.
Recovery	Replace tmnxSecNotifFile with a certificate file that is still valid, or wait until the 'notBefore' time specified in the certificate is reached for the system to recover itself.

66.101 tmnxPkiCertVerificationFailed

Table 1185: tmnxPkiCertVerificationFailed properties

Property name	Value
Application name	SECURITY
Event ID	2044
Event name	tmnxPkiCertVerificationFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.17
Default severity	minor
Message format string	IPsec Tunnel *$tmnxSecNotifTunnelName$* : Certificate *$tmnxSecNotif Cert$* verification failed due to *$tmnxSecNotifFailureReason$*

Property name	Value
Cause	The tmnxPkiCertVerificationFailed notification is generated when an attempt to verify the certificate fails.
Effect	Authentication of the tunnel configured with the certificate will start to fail.
Recovery	Make sure the certificate specified in tmnxSecurityNotifCert exists and is a valid certificate.

66.102 tmnxPkiCRLAfterExpWarning

Table 1186: tmnxPkiCRLAfterExpWarning properties

Property name	Value
Application name	SECURITY
Event ID	2099
Event name	tmnxPkiCRLAfterExpWarning
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.32
Default severity	minor
Message format string	CRL *$tmnxSecNotifFile$* has expired.
Cause	The tmnxPkiCRLAfterExpWarning notification is generated when the CRL (certificate revocation list) indicated in tmnxSecNotifFile has expired.
Effect	The indicated CRL (certificate revocation list) has expired.
Recovery	Replace the indicated file with an updated CRL (certificate revocation list).

66.103 tmnxPkiCRLBeforeExpWarning

Table 1187: tmnxPkiCRLBeforeExpWarning properties

Property name	Value
Application name	SECURITY
Event ID	2098
Event name	tmnxPkiCRLBeforeExpWarning

Property name	Value
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.31
Default severity	minor
Message format string	CRL *$tmnxSecNotifFile$* will expire in *$tmnxPkiExpRemainingHours$* hour(s) and *$tmnxPkiExpRemainingMinutes$* minute(s).
Cause	The tmnxPkiCRLBeforeExpWarning notification is generated when the CRL (certificate revocation list) indicated in tmnxSecNotifFile will expire in the time period indicated by tmnxPkiExpRemainingHours and tmnx PkiExpRemainingMinutes.
Effect	The indicated CRL (certificate revocation list) will expire.
Recovery	Replace the indicated file with an updated CRL (certificate revocation list).

66.104 tmnxPkiCRLExpWarningCleared

Table 1188: tmnxPkiCRLExpWarningCleared properties

Property name	Value
Application name	SECURITY
Event ID	2100
Event name	tmnxPkiCRLExpWarningCleared
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.33
Default severity	minor
Message format string	Expiration warning for CRL *$tmnxSecNotifFile$* is no longer applicable because of the following reason: *$tmnxPkiExpReason$*
Cause	The tmnxPkiCRLExpWarningCleared notification is generated when the expiration warning for the CRL (certificate revocation list) indicated in tmnxSecNotifFile no longer applies because of the reason indicated in tmnxPkiExpReason.
Effect	The indicated CRL (certificate revocation list) is no longer going to expire.
Recovery	None needed.

66.105 tmnxPkiCRLNotYetValid

Table 1189: tmnxPkiCRLNotYetValid properties

Property name	Value
Application name	SECURITY
Event ID	2115
Event name	tmnxPkiCRLNotYetValid
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.50
Default severity	minor
Message format string	CRL *$tmnxSecNotifFile$* is not yet valid.
Cause	The tmnxPkiCRLNotYetValid notification is generated when the CRL (Certificate Revocation List) indicated in tmnxSecNotifFile is not yet valid.
Effect	The CRL is not usable until the 'thisUpdate' time is reached. Unless tmnxPkiCAProfRevokeChk is configured to 'crlOptional (2)', the operational state of the CA-profile (i.e., tmnxPkiCAProfileOperState) remains down until the 'thisUpdate' time is reached.
Recovery	Replace tmnxSecNotifFile with a CRL that is still valid, or wait until the 'thisUpdate' time specified in the CRL is reached for the system to recover itself.

66.106 tmnxPkiFileReadFailed

Table 1190: tmnxPkiFileReadFailed properties

Property name	Value
Application name	SECURITY
Event ID	2043
Event name	tmnxPkiFileReadFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.16
Default severity	minor
Message format string	File *$tmnxSecNotifFile$* read failed due to *$tmnxSecNotifFailure Reason$*

Property name	Value
Cause	The tmnxPkiFileReadFailed notification is generated when an attempt to read the file fails. Reason of the failure is indicated by the tmnxSec NotifFailureReason object.
Effect	Operational status of tunnels configured to use this certificate will be set to 'down'.
Recovery	Make sure the path specified in tmnxSecNotifFile is correct and the file exists.

66.107 tmnxPkiFileWriteFailed

Table 1191: tmnxPkiFileWriteFailed properties

Property name	Value
Application name	SECURITY
Event ID	2109
Event name	tmnxPkiFileWriteFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.41
Default severity	minor
Message format string	File *$tmnxSecNotifFile$* write failed due to *$tmnxSecNotifFailure Reason$*
Cause	The tmnxPkiFileWriteFailed notification is generated when an attempt to write the file fails. Reason for the failure is indicated by the tmnxSec NotifFailureReason object.
Effect	The downloaded file is not saved to disk.
Recovery	Make sure the path specified in tmnxSecNotifFile is correct, file permission is writeable and there is sufficient disk space.

66.108 tmnxSecComputeCertChainFailure

Table 1192: tmnxSecComputeCertChainFailure properties

Property name	Value
Application name	SECURITY
Event ID	2088

Property name	Value
Event name	tmnxSecComputeCertChainFailure
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.24
Default severity	warning
Message format string	Certificate chain of cert file *$tmnxSecNotifFile$* is incomplete due to *$tmnxSecNotifFailureReason$*
Cause	The tmnxSecComputeCertChainFailure notification is generated when a compute chain-failure has occured.
Effect	The chain cannot be built for a configured certificate and the corresponding chain will be empty.
Recovery	Depending on the reason indicated by tmnxSecNotifFailureReason, corrective action should be taken.

66.109 tmnxSecNotifFileReloaded

Table 1193: tmnxSecNotifFileReloaded properties

Property name	Value
Application name	SECURITY
Event ID	2101
Event name	tmnxSecNotifFileReloaded
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.34
Default severity	minor
Message format string	*$tmnxSecNotifFileType$* file " *$tmnxSecNotifFile$*" has been reloaded.
Cause	The tmnxSecNotifFileReloaded notification is generated when the certificate or key indicated in tmnxSecNotifFile is reloaded. tmnxSec NotifFileType indicates whether a certificate or key has been reloaded.
Effect	The indicated certificate or key has been reloaded.
Recovery	None needed.

66.110 tmnxSecNotifKeyChainExpired

Table 1194: tmnxSecNotifKeyChainExpired properties

Property name	Value
Application name	SECURITY
Event ID	2090
Event name	tmnxSecNotifKeyChainExpired
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.26
Default severity	minor
Message format string	Keychain *$tmnxKeyChainName$*: last entry has expired; called by *$tmnxSecNotifOrigProtocol$*
Cause	The tmnxSecNotifKeyChainExpired notification is generated when a protocol instance tries to use a keychain, for which the last key entry has expired.
Effect	N/A
Recovery	N/A

66.111 tmnxSecPwdHistoryFileLoadFailed

Table 1195: tmnxSecPwdHistoryFileLoadFailed properties

Property name	Value
Application name	SECURITY
Event ID	2035
Event name	tmnxSecPwdHistoryFileLoadFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.35
Default severity	minor
Message format string	Failed to load the password history
Cause	The tmnxSecPwdHistoryFileLoadFailed notification is generated when the password history is enabled (tmnxPasswordHistory is not 0) for the first time and the system was unable to load and process the password history. Failure could be due to the following reasons or more: - This is the first time the password history is enabled on this system. - A

Property name	Value
	previous attempt to store the password history failed. - Somebody removed or modified the password history file.
Effect	The system might not be able to compare the new user password with the user's password history from before the last reboot. If tmnxSecPwd HistLoadFailReason is set to 'notFound(1)', a new, empty history file will be created.
Recovery	Investigation might be warranted.

66.112 tmnxSecPwdHistoryFileWriteFailed

Table 1196: tmnxSecPwdHistoryFileWriteFailed properties

Property name	Value
Application name	SECURITY
Event ID	2104
Event name	tmnxSecPwdHistoryFileWriteFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.36
Default severity	minor
Message format string	Failed to write the password history to disk
Cause	The tmnxSecPwdHistoryFileWriteFailed notification is generated when the system is unable to store the password history when an user's password is changed.
Effect	After a reboot, the system might not be able to compare the new user password with the user's password history.
Recovery	Ensure the compact flash is present, and all file permissions are correct.

66.113 tmnxSSHSessionFailed

Table 1197: tmnxSSHSessionFailed properties

Property name	Value
Application name	SECURITY
Event ID	2240

Property name	Value
Event name	tmnxSSHSessionFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.65
Default severity	minor
Message format string	SSH session failed from client *$tmnxSecNotifyAddr$*, reason '*$tmnx SecSSHSessionFailedReason$*'
Cause	The tmnxSSHSessionFailed notification is generated upon the failure of an SSH session establishment. The value of the object tmnxSecNotify AddrType indicates the type of the IP address stored in the object tmnx SecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the source IP address of the user attempting to establish the SSH session. The value of the object tmnxSecSSHSessionFailedReason indicates the reason of the establishment failure.
Effect	SSH session is not established and connection is closed.
Recovery	No recovery action is required.

66.114 tmnxStateChange

Table 1198: tmnxStateChange properties

Property name	Value
Application name	SECURITY
Event ID	2209
Event name	tmnxStateChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.11
Default severity	warning
Message format string	Status of *$tmnxNotifyObjectName$* changed administrative state: *$tmnxNotifyRowAdminState$*, operational state: *$tmnxNotifyRowOper State$*
Cause	There was a change in either the adminstrative or operational state of a MIB table entry.
Effect	N/A
Recovery	No recovery is necessary.

66.115 tmnxSysLicenseExpiresSoon

Table 1199: tmnxSysLicenseExpiresSoon properties

Property name	Value
Application name	SECURITY
Event ID	2092
Event name	tmnxSysLicenseExpiresSoon
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.60
Default severity	major
Message format string	The license installed on *$tmnxHwIndex$* expires *$tmnxSysLicense TimeLeft$*.
Cause	The tmnxSysLicenseExpiresSoon notification is generated when the license is due to expire soon.
Effect	The system will reboot at the end of the time remaining, as specified by tmnxSysLicenseTimeLeft.
Recovery	Configure a valid license file location and file name.

66.116 tmnxSysLicenseInvalid

Table 1200: tmnxSysLicenseInvalid properties

Property name	Value
Application name	SECURITY
Event ID	2091
Event name	tmnxSysLicenseInvalid
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.59
Default severity	major
Message format string	Error - *$tmnxSysLicenseErrorReason$* record. *$tmnxHwIndex$* will *$tmnxSysLicenseErrorAction$ $tmnxSysLicenseTimeLeft$*.
Cause	The tmnxSysLicenseInvalid notification is generated when the license becomes invalid for the reason specified in tmnxSysLicenseError Reason.
Effect	The CPM or system will reboot at the end of the time remaining, as specified by tmnxSysLicenseTimeLeft and tmnxSysLicenseErrorAction.

Property name	Value
Recovery	Configure a valid license file location and file name, given the value of tmnxSysLicenseErrorReason.

66.117 tmnxSysLicenseValid

Table 1201: tmnxSysLicenseValid properties

Property name	Value
Application name	SECURITY
Event ID	2102
Event name	tmnxSysLicenseValid
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.67
Default severity	warning
Message format string	*$tmnxHwIndex$* is running with a valid license.
Cause	The tmnxSysLicenseValid notification is generated once after the system boots up and the license is determined by the system to be valid.
Effect	The system is running with the license specified in tmnxSysLicense Name.
Recovery	No recovery.

66.118 tmnxSystemPasswordChangedByAdmin

Table 1202: tmnxSystemPasswordChangedByAdmin properties

Property name	Value
Application name	SECURITY
Event ID	2248
Event name	tmnxSystemPasswordChangedByAdmin
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.73
Default severity	minor

Property name	Value
Message format string	User '*$tmnxSecNotifyAdminUserName$*' changed the local system ' *$tmnxSecNotifyLocalSystemPassword$*'
Cause	The tmnxSystemPasswordChangedByAdmin notification is generated upon the change of an administrative password by a user with administrative rights. The value of the object tmnxSecNotifyAdmin UserName indicates the user name who changed the password. The value of the object tmnxSecNotifyLocalSystemPassword indicates the administrative password that was changed.
Effect	Users with administrative rights will be able to authenticate with the new password only.
Recovery	No recovery action is required.

66.119 tmnxUserPasswordChangedByAdmin

Table 1203: tmnxUserPasswordChangedByAdmin properties

Property name	Value
Application name	SECURITY
Event ID	2239
Event name	tmnxUserPasswordChangedByAdmin
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.64
Default severity	minor
Message format string	User '*$tmnxSecNotifyAdminUserName$*' changed the password for user ' *$tmnxSecNotifyLocalUserName$*'
Cause	The tmnxUserPasswordChangedByAdmin notification is generated upon the change of a password of a local user by a user with administrative rights. The value of the object tmnxSecNotifyLocal UserName indicates the user name for which the password has been changed. The value of the object tmnxSecNotifyAdminUserName indicates the user name of the user who has changed the password.
Effect	Local user will be able to authenticate to the system with the new password only.
Recovery	No recovery action is required.

66.120 tmnxUsrProfSessionLimitExceeded

Table 1204: tmnxUsrProfSessionLimitExceeded properties

Property name	Value
Application name	SECURITY
Event ID	2111
Event name	tmnxUsrProfSessionLimitExceeded
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.43
Default severity	minor
Message format string	*$tmnxSessionLimitExceededType$* of user profile ' *$tmnxSessionLimitExceededName$*' has been exceeded
Cause	The tmnxUsrProfSessionLimitExceeded notification is generated when an attempt to establish a new user access session is not successful because any of SSH / Telnet / Total session limits defined for the profile of which the user is a member has been exceeded. The value of the object tmnxSessionLimitExceededName indicates the name of the user profile of which the session limit has been exceeded. The value of the object tmnxSessionLimitExceededType indicates the type of the session limit that has been exceeded.
Effect	The user access session has not been established.
Recovery	An administrator may execute one of the following actions in order to allow a successful session establishment: 1) force disconnection of an existing session(s) using 'admin disconnect' CLI command 2) increase the value of the session limit using CLI or SNMP SET operation on the corresponding object in tmnxUserProfileTable 3) revoke the profile membership for the particular user (beware that this action may have impact on user's priviledges)

66.121 user_disconnect

Table 1205: user_disconnect properties

Property name	Value
Application name	SECURITY
Event ID	2015
Event name	user_disconnect
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	major
Message format string	User *$userName$* from *$srcAddr$* logged out by *$disconnectedBy$*
Cause	A user was logged out by the administrator.
Effect	The user's console/telnet/ftp session terminated.
Recovery	No recovery is required

66.122 vRtrIfDcpDynamicConform

Table 1206: vRtrIfDcpDynamicConform properties

Property name	Value
Application name	SECURITY
Event ID	2073
Event name	vRtrIfDcpDynamicConform
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.54
Default severity	warning
Message format string	Network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* newly conformant at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Policer=*$vRtrIfDcpFpProtocol$*(dynamic). Excd count= *$vRtrIfDcpFpDynExcdCount$*
Cause	The vRtrIfDcpDynamicConform notification is generated when the protocol for a particular network-interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected network-interface is now in conformance with the parameters configured for the associated distributed CPU protection policy.
Recovery	There is no recovery required for this notification.

66.123 vRtrIfDcpDynamicEnforceAlloc

Table 1207: vRtrIfDcpDynamicEnforceAlloc properties

Property name	Value
Application name	SECURITY
Event ID	2078
Event name	vRtrIfDcpDynamicEnforceAlloc
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.59
Default severity	warning
Message format string	Dynamic *$vRtrIfDcpFpProtocol$* policers allocated for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*.
Cause	The vRtrIfDcpDynamicEnforceAlloc notification is generated when a dynamic enforcement policer is allocated on a particular network-interface. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The affected network-interface is not in conformance with the configured parameters of the associated distributed CPU protection policy and may be using more resources than expected and cause the system to under-perform.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface may be required.

66.124 vRtrIfDcpDynamicEnforceFreed

Table 1208: vRtrIfDcpDynamicEnforceFreed properties

Property name	Value
Application name	SECURITY
Event ID	2079
Event name	vRtrIfDcpDynamicEnforceFreed
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.60
Default severity	warning
Message format string	Dynamic *$vRtrIfDcpFpProtocol$* policers freed for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTime*

Property name	Value
	EventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Excd count= *$vRtr IfDcpFpDynExcdCount$
Cause	The vRtrIfDcpDynamicEnforceFreed notification is generated when a dynamic enforcement policer is freed on a particular network-interface. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The affected network-interface is now in conformance with the configured parameters of the associated distributed CPU protection policy.
Recovery	There is no recovery required for this notification.

66.125 vRtrIfDcpDynamicExcd

Table 1209: vRtrIfDcpDynamicExcd properties

Property name	Value
Application name	SECURITY
Event ID	2067
Event name	vRtrIfDcpDynamicExcd
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.48
Default severity	warning
Message format string	Non conformant network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* detected at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Policer= *$vRtrIfDcpFpProtocol$*(dynamic). Excd count=*$vRtrIfDcpFpDynExcdCount$*
Cause	The vRtrIfDcpDynamicExcd notification is generated when the protocol on a particular network-interface has been detected as non-conformant to the associated distributed CPU protection policy parameters. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected network-interface may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface may be required.

66.126 vRtrIfDcpDynamicHoldDownEnd

Table 1210: vRtrIfDcpDynamicHoldDownEnd properties

Property name	Value
Application name	SECURITY
Event ID	2071
Event name	vRtrIfDcpDynamicHoldDownEnd
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.52
Default severity	warning
Message format string	Hold-down completed for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Policer= *$vRtrIfDcpFpProtocol$*(dynamic). Excd count=*$vRtrIfDcpFpDynExcdCount$*
Cause	The vRtrIfDcpDynamicHoldDownEnd notification is generated when a particular network-interface completes hold-down period for an exceeding protocol. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The protocol for an affected network-interface will transition to a detection-time countdown after the hold-down period is complete.
Recovery	There is no recovery required for this notification.

66.127 vRtrIfDcpDynamicHoldDownStart

Table 1211: vRtrIfDcpDynamicHoldDownStart properties

Property name	Value
Application name	SECURITY
Event ID	2069
Event name	vRtrIfDcpDynamicHoldDownStart
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.50
Default severity	warning
Message format string	Hold-down started for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtr*

Property name	Value
	IfDCpuProtPolicy$*. Policer= *$vRtrIfDcpFpProtocol$*(dynamic). Excd count=*$vRtrIfDcpFpDynExcdCount$
Cause	The vRtrIfDcpDynamicHoldDownStart notification is generated when a particular network-interface starts hold-down period for an exceeding protocol. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'.
Effect	The protocol will treat all packets as non-conformant during the hold-down period.
Recovery	There is no recovery required for this notification.

66.128 vRtrIfDcpLocMonExcd

Table 1212: vRtrIfDcpLocMonExcd properties

Property name	Value
Application name	SECURITY
Event ID	2074
Event name	vRtrIfDcpLocMonExcd
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.55
Default severity	warning
Message format string	Local monitor *$vRtrIfDcpFpLocMonPlcrName$* for network_if *$vRtr IfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* detected as non-conformant at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProt Policy$*. Excd count= *$vRtrIfDcpFpLocMonExcdCount$*
Cause	The vRtrIfDcpLocMonExcd notification is generated when the local-monitoring-policer for a particular network-interface has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dymanic enforcement policers. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLoc MonPlcrLogEvent is configured to 'verbose'.
Effect	The affected network-interface may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface may be required.

66.129 vRtrIfDcpLocMonExcdAllDynAlloc

Table 1213: vRtrIfDcpLocMonExcdAllDynAlloc properties

Property name	Value
Application name	SECURITY
Event ID	2076
Event name	vRtrIfDcpLocMonExcdAllDynAlloc
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.57
Default severity	warning
Message format string	All dynamic policers allocated for local monitor *$vRtrIfDcpFpLocMonPlcrName$* for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$/$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Excd count=*$vRtrIfDcpFpLocMonExcdCount$*
Cause	The vRtrIfDcpLocMonExcdAllDynAlloc notification is generated when all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for a particular network-interface. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLocMonPlcrLogEvent is configure to 'verbose'.
Effect	The affected network-interface may be using more resources than expected and cause the system to under-perform.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface may be required.

66.130 vRtrIfDcpLocMonExcdAllDynFreed

Table 1214: vRtrIfDcpLocMonExcdAllDynFreed properties

Property name	Value
Application name	SECURITY
Event ID	2077
Event name	vRtrIfDcpLocMonExcdAllDynFreed
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.58
Default severity	warning

Property name	Value
Message format string	All dynamic policers freed for local monitor *$vRtrIfDcpFpLocMon PlcrName$* for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpu ProtPolicy$*.
Cause	The vRtrIfDcpLocMonExcdAllDynFreed notification is generated for a particular network-interface when all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLocMonPlcrLogEvent is configured to 'verbose'.
Effect	The affected network-interface may be using more resources than expected and cause the system to under-perform.
Recovery	There is no recovery required for this notification.

66.131 vRtrIfDcpLocMonExcdDynResource

Table 1215: vRtrIfDcpLocMonExcdDynResource properties

Property name	Value
Application name	SECURITY
Event ID	2075
Event name	vRtrIfDcpLocMonExcdDynResource
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.56
Default severity	warning
Message format string	Local monitor *$vRtrIfDcpFpLocMonPlcrName$* for network_if *$vRtr IfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* detected as non-conformant at *$vRtrIfDcpTimeEventOccured$* and cannot allocate dynamic policers. Policy *$vRtrIfDCpuProtPolicy$*. Excd count=*$vRtr IfDcpFpLocMonExcdCount$*
Cause	The vRtrIfDcpLocMonExcdDynResource notification is generated when the local-monitoring-policer for a particular network-interface has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcements policers associated with the distributed CPU protection policy . This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtLoc MonPlcrLogEvent is configured to 'enable' or 'verbose'.

Property name	Value
Effect	The affected network-interface may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface or to the dynamic enforcement policer pool (TIMETRA-CHASSIS-MIB.mib::tmnxFPDCpuProtDynEnfrcPlcrPool).

66.132 vRtrIfDcpStaticConform

Table 1216: vRtrIfDcpStaticConform properties

Property name	Value
Application name	SECURITY
Event ID	2072
Event name	vRtrIfDcpStaticConform
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.53
Default severity	warning
Message format string	Network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* newly conformant at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Policer=*$vRtrIfDcpFpStaticPlcrName$*(static). Excd count= *$vRtrIfDcpFpStaticExcdCount$*
Cause	The vRtrIfDcpStaticConform notification is generated when the static-policer for a particular network-interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected network-interface is now in conformance with the parameters configured for the associated distributed CPU protection policy.
Recovery	There is no recovery required for this notification.

66.133 vRtrIfDcpStaticExcd

Table 1217: vRtrIfDcpStaticExcd properties

Property name	Value
Application name	SECURITY
Event ID	2066
Event name	vRtrIfDcpStaticExcd
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.47
Default severity	warning
Message format string	Non conformant network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* detected at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Policer= *$vRtrIfDcpFpStaticPlcrName$*(static). Excd count=*$vRtrIfDcpFpStaticExcdCount$*
Cause	The vRtrIfDcpStaticExcd notification is generated when the static-policer on a particular network-interface has been detected as non-conformant to the associated distributed CPU protection policy parameters. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'.
Effect	The affected network-interface may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network.
Recovery	Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface may be required.

66.134 vRtrIfDcpStaticHoldDownEnd

Table 1218: vRtrIfDcpStaticHoldDownEnd properties

Property name	Value
Application name	SECURITY
Event ID	2070
Event name	vRtrIfDcpStaticHoldDownEnd
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.51
Default severity	warning

Property name	Value
Message format string	Hold-down completed for network_if *$vRtrIfIndex$* on fp *$tmnxCard SlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$v RtrIfDCpuProtPolicy$*. Policer= *$vRtrIfDcpFpStaticPlcrName$*(static). Excd count=*$vRtrIfDcpFpStaticExcdCount$*
Cause	The vRtrIfDcpStaticHoldDownEnd notification is generated when a particular network-interface completes hold-down period for an exceeding static-policer. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'verbose'.
Effect	The static-policer for an affected network-interface will transition to a detection-time countdown after the hold-down period is complete.
Recovery	There is no recovery required for this notification.

66.135 vRtrIfDcpStaticHoldDownStart

Table 1219: vRtrIfDcpStaticHoldDownStart properties

Property name	Value
Application name	SECURITY
Event ID	2068
Event name	vRtrIfDcpStaticHoldDownStart
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.49
Default severity	warning
Message format string	Hold-down started for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlot Num$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$v RtrIfDCpuProtPolicy$*. Policer= *$vRtrIfDcpFpStaticPlcrName$*(static). Excd count=*$vRtrIfDcpFpStaticExcdCount$*
Cause	The vRtrIfDcpStaticHoldDownStart notification is generated when a particular network-interface starts hold-down period for an exceeding static-policer. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'verbose'.
Effect	The static-policer will treat all packets as non-conformant during the hold-down period.
Recovery	There is no recovery required for this notification.

67 SFLOW

67.1 tmnxSflowCpEntrySampling

Table 1220: tmnxSflowCpEntrySampling properties

Property name	Value
Application name	SFLOW
Event ID	2001
Event name	tmnxSflowCpEntrySampling
SNMP notification prefix and OID	TIMETRA-SFLOW-MIB.tmnxSflowNotifications.1
Default severity	minor
Message format string	sFlow counter poller sampling - *$tmnxSflowNotifyFlowFailReason$*
Cause	The tmnxSflowCpEntrySampling event is generated when the sampling of an sFlow counter poller is interrupted or started.
Effect	Counter sampling may not be available.
Recovery	N/A

67.2 tmnxSflowPacketTxFailure

Table 1221: tmnxSflowPacketTxFailure properties

Property name	Value
Application name	SFLOW
Event ID	2002
Event name	tmnxSflowPacketTxFailure
SNMP notification prefix and OID	TIMETRA-SFLOW-MIB.tmnxSflowNotifications.2
Default severity	minor
Message format string	sFlow failed to send packet to receiver - *$tmnxSflowNotifyFlowFail Reason$*

Property name	Value
Cause	The tmnxSflowPacketTxFailure event is generated when an sFlow packet fails to transmit from an active sFlow receiver.
Effect	Flow data may be lost.
Recovery	N/A

68 SNMP

68.1 authenticationFailure

Table 1222: authenticationFailure properties

Property name	Value
Application name	SNMP
Event ID	2003
Event name	authenticationFailure
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.5
Default severity	minor
Message format string	Request PDU failed authentication - community = *$subject$*, from IP/UDP *$sourceUDP$*
Cause	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
Effect	The offending PDU is ignored. The requester will time out waiting for a response.
Recovery	If the PDU was from a legitimate requester, then 1) configure the requester to use correct authentication, privacy, MP method, etc. 2) configure the agent to have corresponding access If the PDU was not from a legitimate requester, then use the printed IP address to find the source of the PDU and deal with it appropriately.

68.2 coldStart

Table 1223: coldStart properties

Property name	Value
Application name	SNMP
Event ID	2001

Property name	Value
Event name	coldStart
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.1
Default severity	major
Message format string	SNMP agent cold start
Cause	The SNMP agent was started. The coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
Effect	The system will respond to SNMP requests. The system will send SNMP notifications. Applications will notice counter discontinuities. System configuration may have been altered.
Recovery	To recover from counter discontinuities, re-poll relevent counters to establish a new baseline. Re-poll relevent objects to discover present configuration.

68.3 fallingAlarm

Table 1224: fallingAlarm properties

Property name	Value
Application name	SNMP
Event ID	2102
Event name	fallingAlarm
SNMP notification prefix and OID	RMON-MIB.rmonEventsV2.2
Default severity	major
Message format string	RMON alarm: *$alarmDescription$*
Cause	An RMON alarm entry crossed its falling threshold and generated an event that is configured for sending SNMP traps.
Effect	N/A
Recovery	N/A

68.4 linkDown

Table 1225: linkDown properties

Property name	Value
Application name	SNMP
Event ID	2004
Event name	linkDown
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.3
Default severity	warning
Message format string	Interface *$subject$* is not operational
Cause	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
Effect	The indicated interface is taken down.
Recovery	If the ifAdminStatus is 'down' then the interface state is deliberate and there is no recovery. If the ifAdminStatus is 'up' then try to determine that cause of the interface going down: cable cut, distal end went down, etc.

68.5 linkUp

Table 1226: linkUp properties

Property name	Value
Application name	SNMP
Event ID	2005
Event name	linkUp
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.4
Default severity	warning
Message format string	Interface *$subject$* is operational
Cause	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not

Property name	Value
	into the notPresent state). This other state is indicated by the included value of ifOperStatus.
Effect	The indicated interface is brought up.
Recovery	There is no recovery.

68.6 risingAlarm

Table 1227: risingAlarm properties

Property name	Value
Application name	SNMP
Event ID	2101
Event name	risingAlarm
SNMP notification prefix and OID	RMON-MIB.rmonEventsV2.1
Default severity	major
Message format string	RMON alarm: *$alarmDescription$*
Cause	An RMON alarm entry crossed its rising threshold and generated an event that is configured for sending SNMP traps.
Effect	N/A
Recovery	N/A

68.7 snmpdError

Table 1228: snmpdError properties

Property name	Value
Application name	SNMP
Event ID	2201
Event name	snmpdError
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.21
Default severity	major

Property name	Value
Message format string	SNMP Error: *$tmnxSnmpdErrorMsg$*
Cause	The Snmp daemon detected an error.
Effect	N/A
Recovery	N/A

68.8 warmStart

Table 1229: warmStart properties

Property name	Value
Application name	SNMP
Event ID	2002
Event name	warmStart
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.2
Default severity	major
Message format string	SNMP agent warm start
Cause	The SNMP agent was re-started. A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.
Effect	The system will respond to SNMP requests. The system will send SNMP notifications. Applications will notice counter discontinuities. System configuration has not been altered.
Recovery	To recover from counter discontinuities, re-poll relevent counters to establish a new baseline. There is no need to re-poll relevent objects to discover present configuration.

69 STP

69.1 higherPriorityBridge

Table 1230: higherPriorityBridge properties

Property name	Value
Application name	STP
Event ID	2009
Event name	higherPriorityBridge
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.9
Default severity	warning
Message format string	Bridge *$tmnxCustomerBridgeId$* with root bridge *$tmnxCustomerRootBridgeId$* has higher priority, for service *$svcId$* (customer *$custId$*) on SAP *$sapEncapValue$*
Cause	A customer's device has been configured with a bridge priority equal to zero.
Effect	The SAP that the customer's device is connected through will be blocked.
Recovery	Remove the customer's device or reconfigure the customer's bridge priority with a value greater than zero.

69.2 newRootBridge

Table 1231: newRootBridge properties

Property name	Value
Application name	STP
Event ID	2007
Event name	newRootBridge
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.7
Default severity	warning

Property name	Value
Message format string	New root elected for service *$svcId$* (customer *$custId$*) due to bridge parameter change
Cause	The previous root bridge has been aged out and a new root bridge has been elected.
Effect	The new root bridge creates a new spanning tree topology which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.3 newRootSap

Table 1232: newRootSap properties

Property name	Value
Application name	STP
Event ID	2002
Event name	newRootSap
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.2
Default severity	warning
Message format string	New root elected for service *$svcId$* (customer *$custId$*) due to SAP *$sapEncapValue$*
Cause	The previous root bridge has been aged out and a new root bridge has been elected.
Effect	The new root bridge creates a new spanning tree topology which may denote a loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.4 newRootVcpState

Table 1233: newRootVcpState properties

Property name	Value
Application name	STP

Property name	Value
Event ID	2004
Event name	newRootVcpState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.4
Default severity	warning
Message format string	New root elected for service *$svcId$* (customer *$custId$*) due to VCP state change
Cause	The previous root bridge has been aged out and a new root bridge has been elected.
Effect	The new root bridge creates a new spanning tree topology which may denote a loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss

69.5 pipActiveProtocolChange

Table 1234: pipActiveProtocolChange properties

Property name	Value
Application name	STP
Event ID	2056
Event name	pipActiveProtocolChange
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.42
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) PIP active protocol changed.
Cause	The spanning tree protocol on this PIP changed from RSTP to STP or vise versa.
Effect	N/A
Recovery	No recovery is necessary.

69.6 receivedTCN

Table 1235: receivedTCN properties

Property name	Value
Application name	STP
Event ID	2006
Event name	receivedTCN
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.6
Default severity	warning
Message format string	TCN received for service *$svcId$* (customer *$custId$*) on SAP *$sap EncapValue$*
Cause	A SAP has received a TCN from another bridge.
Effect	This bridge will either have its Config bpdu with topology change flag set if it is a root bridge, or it will pass TCN to its root bridge. Eventually the address aging timer for the forwarding database will be made shorter for a short period of time.
Recovery	No recovery is needed.

69.7 sapActiveProtocolChange

Table 1236: sapActiveProtocolChange properties

Property name	Value
Application name	STP
Event ID	2050
Event name	sapActiveProtocolChange
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.30
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) SAP *$sapPortId$*:*$sapEncap Value$* active protocol changed to *$sapTlsStpOperProtocol$*.
Cause	The spanning tree protocol on this SAP changed from RSTP to STP or vise versa.
Effect	N/A

Property name	Value
Recovery	No recovery is necessary.

69.8 sapEncapDot1d

Table 1237: sapEncapDot1d properties

Property name	Value
Application name	STP
Event ID	2012
Event name	sapEncapDot1d
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.12
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) SAP *$sapEncapValue$* encapsulation changed to 802.1d, bridged with *$tmnxOtherBridgeId$*
Cause	The SAP STP received a BPDU that was 802.1d encapsulated.
Effect	The SAP STP's BPDUs will be 802.1d encapsulated.
Recovery	No recovery is needed.

69.9 sapEncapPVST

Table 1238: sapEncapPVST properties

Property name	Value
Application name	STP
Event ID	2011
Event name	sapEncapPVST
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.11
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) SAP *$sapEncapValue$* encapsulation changed to PVST, bridged with *$tmnxOtherBridgeId$*
Cause	The SAP STP received a BPDU that was PVST encapsulated.

Property name	Value
Effect	The SAP STP's BPDUs will be PVST encapsulated.
Recovery	No recovery is needed.

69.10 tmnxNewCistRegionalRootBridge

Table 1239: tmnxNewCistRegionalRootBridge properties

Property name	Value
Application name	STP
Event ID	2021
Event name	tmnxNewCistRegionalRootBridge
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.33
Default severity	warning
Message format string	New *$svcStpRegionalName$*root *$svcTlsStpCistRegionalRoot$* elected in service *$svcId$*
Cause	A STP selected a new regional root for the CIST.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

69.11 tmnxNewMstiRegionalRootBridge

Table 1240: tmnxNewMstiRegionalRootBridge properties

Property name	Value
Application name	STP
Event ID	2022
Event name	tmnxNewMstiRegionalRootBridge
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.34
Default severity	warning
Message format string	New MSTI regional root *$tlsMstiRegionalRoot$* elected in service *$svc Id$*. Msti-InstanceId: *$svcMstiInstanceId$*

Property name	Value
Cause	A STP selected a new regional root for the MSTI.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

69.12 tmnxPipStpExcepCondStateChng

Table 1241: tmnxPipStpExcepCondStateChng properties

Property name	Value
Application name	STP
Event ID	2055
Event name	tmnxPipStpExcepCondStateChng
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.41
Default severity	warning
Message format string	The stp exception condition state for service *$svcId$* (customer *$custId $*) on PIP has chnaged to *$tlsPipStpException$*
Cause	The STP exception state has changed.
Effect	N/A
Recovery	N/A

69.13 tmnxSapStpExcepCondStateChng

Table 1242: tmnxSapStpExcepCondStateChng properties

Property name	Value
Application name	STP
Event ID	2025
Event name	tmnxSapStpExcepCondStateChng
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.37
Default severity	warning

Property name	Value
Message format string	The stp exception condition state for service *$svcId$* (customer *$custId $*) on SAP *$sapEncapValue$* has chnaged to *$sapTlsStpException$*
Cause	A STP exception state has changed.
Effect	N/A
Recovery	N/A

69.14 tmnxSdpBndStpExcepCondStateChng

Table 1243: tmnxSdpBndStpExcepCondStateChng properties

Property name	Value
Application name	STP
Event ID	2026
Event name	tmnxSdpBndStpExcepCondStateChng
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.38
Default severity	warning
Message format string	The Stp Exception condition has changed to *$sdpBindTlsStpException $* in service *$svcId$* (customer *$custId$*) on SDP Bind *$sdpBindId$*
Cause	The STP exception condition has changed on an SDP Binding."
Effect	N/A
Recovery	N/A

69.15 tmnxStpMeshNotInMstRegion

Table 1244: tmnxStpMeshNotInMstRegion properties

Property name	Value
Application name	STP
Event ID	2024
Event name	tmnxStpMeshNotInMstRegion
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.36

Property name	Value
Default severity	warning
Message format string	A MSTP BPDU from outside the MST region is received on mesh SDP *$sdpBindId$* in service *$svcId$*. The mesh will not become operational!
Cause	A MSTP BPDU from outside the MST region is received on the mesh SDP.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

69.16 tmnxStpRootGuardViolation

Table 1245: tmnxStpRootGuardViolation properties

Property name	Value
Application name	STP
Event ID	2023
Event name	tmnxStpRootGuardViolation
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.35
Default severity	warning
Message format string	A root-guard violation is detected for service *$svcId$* on SAP *$sap EncapValue$*
Cause	A STP detects a root-guard violation.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

69.17 tmnxSvcNewRootSdpBind

Table 1246: tmnxSvcNewRootSdpBind properties

Property name	Value
Application name	STP
Event ID	2015

Property name	Value
Event name	tmnxSvcNewRootSdpBind
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.15
Default severity	warning
Message format string	New root bridge *$svcTlsStpDesignatedRoot$* elected for service *$svcId $* (customer *$custId$*) due to SDP Bind *$sdpBindId$*
Cause	The previous root bridge has been aged out and a new root bridge has been elected.
Effect	The new root bridge creates a new spanning tree topology which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.18 tmnxSvcSdpActiveProtocolChange

Table 1247: tmnxSvcSdpActiveProtocolChange properties

Property name	Value
Application name	STP
Event ID	2051
Event name	tmnxSvcSdpActiveProtocolChange
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.31
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) SDP Bind *$sdpBindId$* active changed to *$sdpBindTlsStpOperProtocol$*.
Cause	The spanning tree protocol on an SDP changed from RSTP to STP or vise versa.
Effect	N/A
Recovery	No recovery is necessary.

69.19 tmnxSvcSdpBindEncapDot1d

Table 1248: tmnxSvcSdpBindEncapDot1d properties

Property name	Value
Application name	STP
Event ID	2020
Event name	tmnxSvcSdpBindEncapDot1d
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.20
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) SDP Bind *$sdpBindId$* encapsulation changed to 802.1d, bridged with *$tmnxOtherBridgeId$*
Cause	The SDP Binding STP received a BPDU that was 802.1d encapsulated.
Effect	The SDP Binding STP's BPDUs will be 802.1d encapsulated.
Recovery	No recovery is needed.

69.20 tmnxSvcSdpBindEncapPVST

Table 1249: tmnxSvcSdpBindEncapPVST properties

Property name	Value
Application name	STP
Event ID	2019
Event name	tmnxSvcSdpBindEncapPVST
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.19
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*) SDP Bind *$sdpBindId$* encapsulation changed to PVST, bridged with *$tmnxOtherBridgeId$*
Cause	The SDP Binding STP received a BPDU that was PVST encapsulated.
Effect	The SDP Binding STP's BPDUs will be PVST encapsulated.
Recovery	No recovery is needed.

69.21 tmnxSvcSdpBindRcvdHigherBriPrio

Table 1250: tmnxSvcSdpBindRcvdHigherBriPrio properties

Property name	Value
Application name	STP
Event ID	2018
Event name	tmnxSvcSdpBindRcvdHigherBriPrio
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.18
Default severity	warning
Message format string	Bridge *$tmnxCustomerBridgeId$* with root bridge *$tmnxCustomerRoot BridgeId$* has higher priority, for service *$svcId$* (customer *$custId$*) on SDP Bind *$sdpBindId$*
Cause	A customer's device has been configured with a bridge priority equal to zero.
Effect	The SDP Binding that the customer's device is connected through will be blocked.
Recovery	Remove the customer's device or reconfigure the customer's bridge priority with a value greater than zero.

69.22 tmnxSvcSdpBindRcvdTCN

Table 1251: tmnxSvcSdpBindRcvdTCN properties

Property name	Value
Application name	STP
Event ID	2017
Event name	tmnxSvcSdpBindRcvdTCN
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.17
Default severity	warning
Message format string	TCN received for service *$svcId$* (customer *$custId$*) on SDP Bind *$sdpBindId$*
Cause	A SDP Binding has received TCN from another bridge.

Property name	Value
Effect	This bridge will either have its Config bpdu with topology change flag set if it is a root bridge, or it will pass TCN to its root bridge. Eventually the address aging timer for the forwarding database will be made shorter for a short period of time.
Recovery	No recovery is needed.

69.23 tmnxSvcTopoChgSdpBindMajorState

Table 1252: tmnxSvcTopoChgSdpBindMajorState properties

Property name	Value
Application name	STP
Event ID	2014
Event name	tmnxSvcTopoChgSdpBindMajorState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.14
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to SDP Bind *$sdpBindId$* state change from *$tmnxOldSdpBindTlsStpPortState $* to *$sdpBindTlsStpPortState$*
Cause	A SDP Binding has transitioned its state from learning to forwarding or from forwarding to blocking or broken.
Effect	The spanning tree topology has been modified which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.24 tmnxSvcTopoChgSdpBindState

Table 1253: tmnxSvcTopoChgSdpBindState properties

Property name	Value
Application name	STP
Event ID	2016
Event name	tmnxSvcTopoChgSdpBindState

Property name	Value
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.16
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to SDP Bind *$sdpBindId$* state change from *$tmnxOldSdpBindTlsStpPortState $* to *$sdpBindTlsStpPortState$*
Cause	A SDP Binding has transitioned state to blocking or broken from a state other than forwarding. This event complements what is not covered by topologyChangeSapMajorState.
Effect	The spanning tree topology has been modified which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.25 topologyChangePipMajorState

Table 1254: topologyChangePipMajorState properties

Property name	Value
Application name	STP
Event ID	2053
Event name	topologyChangePipMajorState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.39
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to PIP major state change
Cause	PIP has transitioned its state from learning to forwarding or from forwarding to blocking or broken.
Effect	The spanning tree topology has been modified which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss

69.26 topologyChangePipState

Table 1255: topologyChangePipState properties

Property name	Value
Application name	STP
Event ID	2054
Event name	topologyChangePipState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.40
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to PIP state change
Cause	PIP has transitioned state to blocking or broken from a state other than forwarding. This event complements what is not covered by topology ChangePipMajorState.
Effect	The spanning tree topology has been modified which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine severity of connectivity loss.

69.27 topologyChangeSapMajorState

Table 1256: topologyChangeSapMajorState properties

Property name	Value
Application name	STP
Event ID	2001
Event name	topologyChangeSapMajorState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.1
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to SAP *$sapEncapValue$* major state change
Cause	A SAP has transitioned its state from learning to forwarding or from forwarding to blocking or broken.

Property name	Value
Effect	The spanning tree topology has been modified which may denote loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.28 topologyChangeSapState

Table 1257: topologyChangeSapState properties

Property name	Value
Application name	STP
Event ID	2005
Event name	topologyChangeSapState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.5
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to SAP *$sapEncapValue$* state change
Cause	A SAP has transitioned state to blocking or broken from a state other than forwarding. This event complements what is not covered by topologyChangeSapMajorState.
Effect	The spanning tree topology has been modified which may denote a loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.29 topologyChangeVcpState

Table 1258: topologyChangeVcpState properties

Property name	Value
Application name	STP
Event ID	2003
Event name	topologyChangeVcpState

Property name	Value
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.3
Default severity	warning
Message format string	Topology change for service *$svcId$* (customer *$custId$*) due to VCP state change to *$tmnxVcpState$*
Cause	A VCP has transitioned its state from disabled to forwarding or from forwarding to disabled.
Effect	The spanning tree topology has been modified which may denote a loss of customer access or redundancy.
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

69.30 unacknowledgedTCN

Table 1259: unacknowledgedTCN properties

Property name	Value
Application name	STP
Event ID	2008
Event name	unacknowledgedTCN
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.8
Default severity	warning
Message format string	TCN sent for service *$svcId$* (customer *$custId$*) to SDP *$sdpId$* is unacknowledged
Cause	A TCN sent towards the root bridge on the root port (SAP) has not been acknowledged within allowed time.
Effect	A portion of the spanning tree topology may not have been notified that a topology change has taken place. FDB tables on some devices may take significantly longer to represent the new distribution of layer-2 addresses.
Recovery	Diagnose this device and devices towards the root bridge for STP issues.

69.31 vcpActiveProtocolChange

Table 1260: vcpActiveProtocolChange properties

Property name	Value
Application name	STP
Event ID	2052
Event name	vcpActiveProtocolChange
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.32
Default severity	minor
Message format string	Service *$svcId$* (customer *$custId$*)VCP Active protocol changed to *$svcTlsStpVcpOperProtocol$*.
Cause	The spanning tree protocol on a VCP changed from RSTP to STP or vise versa.
Effect	N/A
Recovery	No recovery is necessary.

70 SVCMGR

70.1 aluSapCemActiveMultipathStateChg

Table 1261: aluSapCemActiveMultipathStateChg properties

Property name	Value
Application name	SVCMGR
Event ID	2001
Event name	aluSapCemActiveMultipathStateChg
SNMP notification prefix and OID	ALU-SERVICE-MIB.aluServNotifyObjs.2
Default severity	minor
Message format string	TODO
Cause	Generated if aluSapCemStatsActiveMultipathStateChgCnt increased since the last poll.
Effect	N/A
Recovery	N/A

70.2 dynamicSdpBindConfigChanged

Table 1262: dynamicSdpBindConfigChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2320
Event name	dynamicSdpBindConfigChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.25
Default severity	major
Message format string	The configuration for dynamic *$dynamicSdpOrigin$* SDP Bind *$svcL2RteSdpBindId$ $sdpMSPwPeId$* was *$dynamicSdpStatus$*.

Property name	Value
Cause	The dynamicSdpBindConfigChanged notification is generated when a dynamic SDP Bind is 'created', 'modified', or 'deleted'. New state of the SDP Bind is indicated by the value of dynamicSdpStatus. The affected SDP is indicated by the value of 'sdpId' or by Spoke-SDP FEC identifier 'sdpMSPwPeId'.
Effect	This is an informational notification. Depending on the type of change, new layer-2 route may have been created, modified or deleted.
Recovery	No recovery action is required."

70.3 dynamicSdpBindCreationFailed

Table 1263: dynamicSdpBindCreationFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2322
Event name	dynamicSdpBindCreationFailed
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.27
Default severity	major
Message format string	The system failed to create a dynamic *$dynamicSdpOrigin$* SDP Bind on SDP *$sdpId$* for the following reason: *$dynamicSdpBindCreation Error$*.
Cause	The system failed to create a dynamic SDP Bind.
Effect	N/A
Recovery	N/A

70.4 dynamicSdpConfigChanged

Table 1264: dynamicSdpConfigChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2319

Property name	Value
Event name	dynamicSdpConfigChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.24
Default severity	major
Message format string	The configuration for dynamic *$dynamicSdpOrigin$* SDP *$sdpId$* was *$dynamicSdpStatus$*.
Cause	A dynamic SDP was 'created', 'modified', or 'deleted'.
Effect	N/A
Recovery	N/A

70.5 dynamicSdpCreationFailed

Table 1265: dynamicSdpCreationFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2321
Event name	dynamicSdpCreationFailed
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.26
Default severity	major
Message format string	The system failed to create a dynamic *$dynamicSdpOrigin$* SDP for the following reason: *$dynamicSdpCreationError$*.
Cause	The system failed to create a dynamic SDP.
Effect	N/A
Recovery	N/A

70.6 hostConnectivityLost

Table 1266: hostConnectivityLost properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2206
Event name	hostConnectivityLost
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.13
Default severity	warning
Message format string	host connectivity lost on *$sapEncapValue$* in service *$svcId$* for inet Addr = *$hostConnectivityCiAddr$*, chAddr= *$hostConnectivityChAddr$*, verify-addr=*$sapNotifyIpAddr$*.
Cause	The system lost the conectivity with a host.
Effect	N/A
Recovery	N/A

70.7 hostConnectivityRestored

Table 1267: hostConnectivityRestored properties

Property name	Value
Application name	SVCMGR
Event ID	2207
Event name	hostConnectivityRestored
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.14
Default severity	warning
Message format string	host connectivity restored on *$sapEncapValue$* in service *$svcId$*, for inetAddr = *$hostConnectivityCiAddr$*, chAddr= *$hostConnectivity ChAddr$*, verify-addr=*$sapNotifyIpAddr$*.
Cause	Connectivity to a host has been restored.
Effect	N/A
Recovery	N/A

70.8 iesIfStatusChanged

Table 1268: iesIfStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2108
Event name	iesIfStatusChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.8
Default severity	minor
Message format string	Status of interface *$iesIfName$* in service *$svcId$* (customer *$custId$*) changed to admin= *$iesIfAdminStatus$* oper=*$iesIfOperStatus$*
Cause	There was a change in the administrative or operating status of an IES interface.
Effect	N/A
Recovery	N/A

70.9 msapCreationFailure

Table 1269: msapCreationFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2214
Event name	msapCreationFailure
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.26
Default severity	minor
Message format string	The system could not create a Managed SAP: *$sapNotifyEncapValue $* MAC:*$sapTlsNotifyMacAddr$*, Capturing SAP: *$sapEncapValue$*, service:*$svcId$*. Description: *$svcManagedSapCreationError$*
Cause	The system failed to create a managed SAP.
Effect	N/A
Recovery	N/A

70.10 msapStateChanged

Table 1270: msapStateChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2213
Event name	msapStateChanged
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.25
Default severity	minor
Message format string	Managed SAP, *$sapEncapValue$* in service *$svcId$*, has been *$msap Status$*
Cause	A managed SAP was 'created', 'modified', or 'deleted'.
Effect	N/A
Recovery	N/A

70.11 sapAtmPppNcpFailure

Table 1271: sapAtmPppNcpFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2540
Event name	sapAtmPppNcpFailure
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.32
Default severity	warning
Message format string	ATM PPP *$sapPppNcpFailureProtocol$* phase failure for user *$sap NotifyName$* on SAP *$sapEncapValue$* in service *$svcId$ - $sapNotify Reason$*
Cause	The sapAtmPppNcpFailure notification indicates that there is a NCP phase setup problem. The problem is described in the object sapNotify Reason. The PPP user name is specified in the sapNotifyName.

Property name	Value
Effect	The user that attempted to set up the PPP session cannot establish the desired connection.
Recovery	Depending on the reason indicated by sapNotifyReason, corrective action may be necessary. However, it is possible that the failure is caused by the user's equipment configuration or by erroneous input by the user.

70.12 sapAtmPppSessionFailure

Table 1272: sapAtmPppSessionFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2539
Event name	sapAtmPppSessionFailure
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.31
Default severity	warning
Message format string	ATM PPP session failure for user *$sapNotifyName$* on SAP *$sapEncapValue$* in service *$svcId$* - *$sapNotifyReason$*
Cause	The sapAtmPppSessionFailure notification indicates that the system could not create a new PPPoA session. The problem is described in the object sapNotifyReason. The PPP user name is specified in the sapNotifyName.
Effect	The user that attempted to set up the PPP session cannot establish the desired connection.
Recovery	Depending on the reason indicated by sapNotifyReason, corrective action may be necessary. However, it is possible that the failure is caused by the user's equipment configuration or by erroneous input by the user.

70.13 sapCemPacketDefectAlarm

Table 1273: sapCemPacketDefectAlarm properties

Property name	Value
Application name	SVCMGR
Event ID	2211
Event name	sapCemPacketDefectAlarm
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.23
Default severity	minor
Message format string	SAP *$sapEncapValue$* in service *$svcId$* (customer *$custId$*): Alarm '*$sapCemReportAlarmStatus$*' Set.
Cause	The CEM SAP experienced a persistent defect over a 3 second window.
Effect	N/A
Recovery	N/A

70.14 sapCemPacketDefectAlarmClear

Table 1274: sapCemPacketDefectAlarmClear properties

Property name	Value
Application name	SVCMGR
Event ID	2212
Event name	sapCemPacketDefectAlarmClear
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.24
Default severity	minor
Message format string	SAP *$sapEncapValue$* in service *$svcId$* (customer *$custId$*): Alarm '*$sapCemReportAlarmStatus$*' Cleared.
Cause	The CEM SAP no longer experiences 30 percent or more packet errors in a 10 second window.
Effect	N/A
Recovery	N/A

70.15 sapEthLoopbackStarted

Table 1275: sapEthLoopbackStarted properties

Property name	Value
Application name	SVCMGR
Event ID	2230
Event name	sapEthLoopbackStarted
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.54
Default severity	minor
Message format string	Started loopback on SAP *$sapEncapValue$ $sapEthLoopbackMode$* in service *$svcId$*.
Cause	The sapEthLoopbackStarted notification is generated when the SAP is placed into loopback.
Effect	This notification is informational only.
Recovery	N/A

70.16 sapEthLoopbackStopped

Table 1276: sapEthLoopbackStopped properties

Property name	Value
Application name	SVCMGR
Event ID	2231
Event name	sapEthLoopbackStopped
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.55
Default severity	minor
Message format string	Stopped loopback on SAP *$sapEncapValue$ $sapEthLoopbackMode$* in service *$svcId$*.
Cause	The sapEthLoopbackStopped notification is generated when the SAP is removed from loopback.
Effect	This notification is informational only.

Property name	Value
Recovery	N/A

70.17 sapHostBGPPeeringSetupFailed

Table 1277: sapHostBGPPeeringSetupFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2526
Event name	sapHostBGPPeeringSetupFailed
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.27
Default severity	minor
Message format string	The system could not set up a BGP Neighbor for host *$sapBGPPeeringHostIpAddr$* on SAP:*$sapEncapValue$*, service: *$svcId$*. BGP peering attributes discarded: *$sapBGPPeeringAttrDiscarded$*. Description: *$sapBGPPeeringNotifDescription$*
Cause	The system was unable to create a BGP neighbor and set up BGP peering for a given host. Possible causes are: - no ESM (Enhanced Subscriber Management) configured on the SAP - a wrong anti-spoof type is configured on the SAP (should be nh-mac) - the group interface is not operational - the host is not forwarding - the host is in dual homed setup - the system limit of BGP neighbors is reached - one or more BGP peering attributes attributes are invalid - BGP is not configured in the service - not enough memory.
Effect	No BGP neighbor was created for this host. BPP peering attributes might have been deleted; whether or not they were, is indicated by the value of sapBGPPeeringAttrDiscarded.
Recovery	N/A

70.18 sapHostRipListenerSetupFailed

Table 1278: sapHostRipListenerSetupFailed properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2065
Event name	sapHostRipListenerSetupFailed
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.57
Default severity	minor
Message format string	The system could not set up a RIP lsistener for host *$sapRipListener HostIpAddr$* on SAP:*$sapEncapValue$*, service: *$svcId$*.Description: *$sapRipListenerNotifDescription$*
Cause	To be documented
Effect	To be documented
Recovery	No recovery is required on this system.

70.19 sapIfIgnorePortStateStart

Table 1279: sapIfIgnorePortStateStart properties

Property name	Value
Application name	SVCMGR
Event ID	2245
Event name	sapIfIgnorePortStateStart
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.61
Default severity	warning
Message format string	Ignoring SAP port state in service: *$svcId$* for IP interface *$sapNotify IfName$*.
Cause	The sapIfIgnorePortStateStart notification is generated when system starts to ignore non-operational state of the port associated with the IP interface.
Effect	This notification is informational only.
Recovery	Set sapL3LoopbackRowStatus to 'destroy' to stop this.

70.20 sapIfIgnorePortStateStop

Table 1280: sapIfIgnorePortStateStop properties

Property name	Value
Application name	SVCMGR
Event ID	2246
Event name	sapIfIgnorePortStateStop
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.62
Default severity	warning
Message format string	Stopped ignoring SAP port state in service: *$svcId$* for IP interface *$sapNotifyIfName$*.
Cause	The sapIfIgnorePortStateStop notification is generated when system stops to ignore non-operational state of the port associated with the IP interface.
Effect	This notification is informational only.
Recovery	None required.

70.21 sapIpipeCeIpAddrChange

Table 1281: sapIpipeCeIpAddrChange properties

Property name	Value
Application name	SVCMGR
Event ID	2543
Event name	sapIpipeCeIpAddrChange
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.33
Default severity	minor
Message format string	CE IP address *$sapIpipeCeIpAddress$* is discovered on Ipipe SAP *$sapEncapValue$* in service *$svcId$*.
Cause	The sapIpipeCeIpAddrChange notification indicates that an IP address has been discovered for the local end host of a specified IPIPE SAP. The IP address type is specified by sapIpipeCeIpAddrType. The IP address is specified by sapIpipeCeIpAddress.

Property name	Value
Effect	The IP address specified by sapIpipeCeIpAddress and of type sapIpipe CeIpAddrType has been discovered for the local end host.
Recovery	No action is required.

70.22 sapPortStateChangeProcessed

Table 1282: sapPortStateChangeProcessed properties

Property name	Value
Application name	SVCMGR
Event ID	2210
Event name	sapPortStateChangeProcessed
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.21
Default severity	major
Message format string	Processing of an access port state change event is finished and the status of all affected SAPs on port *$sapNotifyPortId$* has been updated.
Cause	The processing of all SAPs affected by a port state change event, link Up or linkDown, has finished.
Effect	When a port changes state as a result of a linkUp or linkDown event, all SAPs associated with that port also change state. The sapStatus Changed events are suppressed and when the processing of state changes for all SAPs associated with the port is finished, a single sap PortStateChangeProcessed event is generated.
Recovery	N/A

70.23 sapReceivedProtSrcMac

Table 1283: sapReceivedProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2208
Event name	sapReceivedProtSrcMac

Property name	Value
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.15
Default severity	minor
Message format string	Protected MAC *$protectedMacForNotify$* received on SAP *$sapEncap Value$* in service *$svcId$*.
Cause	A protected source MAC was received on a TLS SAP.
Effect	N/A
Recovery	N/A

70.24 sapStatusChanged

Table 1284: sapStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2203
Event name	sapStatusChanged
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.3
Default severity	minor
Message format string	Status of SAP *$sapEncapValue$* in service *$svcId$* (customer *$cust Id$*) changed to admin= *$sapAdminStatus$* oper=*$sapOperStatus$* flags=*$sapOperFlags$*
Cause	There was a change in the administrative or operating status of an SAP. Notice that this event is not generated when the SAP operating status change was caused by an operating status change on the associated access port."
Effect	N/A
Recovery	N/A

70.25 sapTlsDataSapInstStatusChgd

Table 1285: sapTlsDataSapInstStatusChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2532
Event name	sapTlsDataSapInstStatusChgd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.28
Default severity	minor
Message format string	Data SAP instantiation status for service *$svcId$* SAP *$sapEncapValue $* changed to *$sapTlsDataSapInstStatus$* with last-error: *$sapTlsData SapInstLastErr$*
Cause	Data SAP instantiation status changed
Effect	N/A
Recovery	N/A

70.26 sapTlsMacAddrLimitAlarmCleared

Table 1286: sapTlsMacAddrLimitAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2205
Event name	sapTlsMacAddrLimitAlarmCleared
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.5
Default severity	minor
Message format string	Number of MAC addr learned by SAP *$sapEncapValue$* in service *$svcId$* dropped below the LowWaterMark.
Cause	The number of MAC addresses stored in the FDB for this SAP dropped below the low watermark.
Effect	N/A
Recovery	N/A

70.27 sapTlsMacAddrLimitAlarmRaised

Table 1287: sapTlsMacAddrLimitAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2204
Event name	sapTlsMacAddrLimitAlarmRaised
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.4
Default severity	minor
Message format string	Number of MAC addr learned by SAP *$sapEncapValue$* in service *$svcId$* reached the HighWaterMark.
Cause	The number of MAC addresses stored in the FDB for this SAP exceeded the the high watermark."
Effect	N/A
Recovery	N/A

70.28 sapTlsMacMoveExceeded

Table 1288: sapTlsMacMoveExceeded properties

Property name	Value
Application name	SVCMGR
Event ID	2209
Event name	sapTlsMacMoveExceeded
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.17
Default severity	minor
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sapTls NotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* and will retry in *$sapTlsMacMoveNextUpTime$* seconds (retries left= *$sapTlsMacMove RateExcdLeft$* admin=*$sapAdminStatus$* oper=*$sapOperStatus$*) - detected on SAP *$sapEncapValue$*
Cause	The TLS svcTlsMacMoveMaxRate has been exceeded for the SAP.

Property name	Value
Effect	The interface will be brought down and then brought back up automatically in sapTlsMacMoveNextUpTime seconds if retries are left as indicated by sapTlsMacMoveRateExcdLeft.
Recovery	If there are retries left, as indicated by sapTlsMacMoveRateExcd Left, the interface will be brought back up automatically in sapTlsMac MoveNextUpTime seconds. If no retries are left, the interface must be manually brought back up by an adminstrator.

70.29 sapTlsMacMoveExceedNonBlock

Table 1289: sapTlsMacMoveExceedNonBlock properties

Property name	Value
Application name	SVCMGR
Event ID	2229
Event name	sapTlsMacMoveExceedNonBlock
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.53
Default severity	minor
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sapTls NotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* - detected on SAP *$sapEncapValue$*
Cause	The sapTlsMacMoveExceedNonBlock notification is generated when the SAP exceeds the TLS svcTlsMacMoveMaxRate when sapTlsLimit MacMove is set to 'nonBlocking'.In case of Provider Backbone Bridging (PBB), if the MAC address that exceeds the rate is ISID-VPLS(iVpls) FDB and sap binding that detects the move is in Backbone-VPLS(b Vpls), the notification will be generated with svcId, custId of I-VPLS and B-VPLS sapId.
Effect	This notification is informational only.
Recovery	User can adjust the value of svcTlsMacMoveMaxRate to reduce the frequency of this notification.

70.30 sapTunnelEncapIpMtuTooSmall

Table 1290: sapTunnelEncapIpMtuTooSmall properties

Property name	Value
Application name	SVCMGR
Event ID	2232
Event name	sapTunnelEncapIpMtuTooSmall
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.56
Default severity	warning
Message format string	Addition of tunnel encapsulation at IP tunnel *$sapTunnelNotifyName $* on SAP:*$sapEncapValue$*, service:*$svcId$* with configured MTU of *$sapTunnelNotifyConfigIpMtu$*, having encapsulated MTU of *$sapTunnelNotifyConfigEncapIpMtu$* has an overhead of *$sapTunnelNotifyEncapOverhead$*.
Cause	The sapTunnelEncapIpMtuTooSmall notification is generated when the addition of tunnel encapsulation to a packet at or near the IP Tunnel's configured IP MTU may cause it to exceed the tunnel's configured encapsulated IP MTU.
Effect	The pre-encapsulated packet may be fragmented, and will require reassembly by the tunnel remote endpoint, causing a performance impact.
Recovery	Configured IP MTU and/or encapsulated IP MTU may need to be changed depending on the size of the encapsulation overhead as indicated in 'sapTunnelNotifyEncapOverhead', and the transmission capabilities of the tunnel's transport network.

70.31 sapTunnelStateChange

Table 1291: sapTunnelStateChange properties

Property name	Value
Application name	SVCMGR
Event ID	2535
Event name	sapTunnelStateChange
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.30
Default severity	minor

Property name	Value
Message format string	Operational State of Tunnel *$sapTunnelNotifyName$* has changed to *$sapTunnelNotifyState$* due to *$sapTunnelNotifyReason$*
Cause	The trap sapTunnelStateChange is sent when IPsec/GRE tunnel indicated by sapTunnelNotifyName changes state to 'down' due to sap TunnelNotifyReason.
Effect	IPsec/GRE tunnel associated with the SAP will remain in this state until a corrective action is taken.
Recovery	Depending on the reason indicated by sapTunnelNotifyReason, corrective action should be taken.

70.32 sdpBandwidthOverbooked

Table 1292: sdpBandwidthOverbooked properties

Property name	Value
Application name	SVCMGR
Event ID	2317
Event name	sdpBandwidthOverbooked
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.22
Default severity	major
Message format string	The booked bandwidth *$sdpBookedBandwidth$* of SDP *$sdpId$* has exceeded the max bookable bandwidth *$sdpMaxBookableBandwidth$*.
Cause	The booked bandwidth that has been allocated to the SDP bindings exceeded the maximum bookable bandwidth.
Effect	N/A
Recovery	N/A

70.33 sdpBindEthLoopbackStarted

Table 1293: sdpBindEthLoopbackStarted properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2328
Event name	sdpBindEthLoopbackStarted
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.33
Default severity	minor
Message format string	Started loopback on SDP binding *$sdpBindId$ $sdpBindEthLoopbackMode$* in service *$svcId$*.
Cause	The sdpBindEthLoopbackStarted notification is generated when the SDP binding is placed into loopback.
Effect	This notification is informational only.
Recovery	N/A

70.34 sdpBindEthLoopbackStopped

Table 1294: sdpBindEthLoopbackStopped properties

Property name	Value
Application name	SVCMGR
Event ID	2329
Event name	sdpBindEthLoopbackStopped
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.34
Default severity	minor
Message format string	Stopped loopback on SDP binding *$sdpBindId$ $sdpBindEthLoopbackMode$* in service *$svcId$*.
Cause	The sdpBindEthLoopbackStopped notification is generated when the SDP binding is removed from loopback.
Effect	This notification is informational only.
Recovery	N/A

70.35 sdpBindInsufficientBandwidth

Table 1295: sdpBindInsufficientBandwidth properties

Property name	Value
Application name	SVCMGR
Event ID	2318
Event name	sdpBindInsufficientBandwidth
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.23
Default severity	major
Message format string	The available bandwidth *$sdpAvailableBandwidth$* of SDP cannot satisfy the bandwidth *$sdpBindAdminBandwidth$* required by the SDP Bind *$sdpBindId$*.
Cause	The available bandwidth of the SDP is insufficient to satisfy the bandwidth requirement required by a SDP binding.
Effect	N/A
Recovery	N/A

70.36 sdpBindIpipeCeIpAddressChange

Table 1296: sdpBindIpipeCeIpAddressChange properties

Property name	Value
Application name	SVCMGR
Event ID	2324
Event name	sdpBindIpipeCeIpAddressChange
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.29
Default severity	minor
Message format string	CE IP address *$sdpBindIpipeCeIpAddress$* is discovered on Ipipe SDP bind *$sdpBindId$* in service *$svcId$*.
Cause	The sdpBindIpipeCeIpAddressChange notification indicates an IP address has been discovered for the far end CE device on a specified IPIPE SDP. The type of IP address is specified by sdpBindIpipeCeIp AddrType. The IP address is specified by sdpBindIpipeCeIpAddress.

Property name	Value
Effect	The IP address specified by sdpBindIpipeCeIpAddress and of type sdp BindIpipeCeIpAddrType has been discovered on the remote CE device.
Recovery	No action is required.

70.37 sdpBindPwLocalStatusBitsChanged

Table 1297: sdpBindPwLocalStatusBitsChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2326
Event name	sdpBindPwLocalStatusBitsChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.31
Default severity	minor
Message format string	Status of SDP Bind *$sdpBindId$* in service *$svcId$* (customer *$custId $*) local PW status bits changed to *$sdpBindPwLocalStatusBitsString$*
Cause	The sdpBindPwLocalStatusBitsChanged notification is generated when there is a change in the local PW status bits.
Effect	Based on the change in the sdpBindPwLocalStatusBits traffic on the SDP-BIND may be impacted.
Recovery	Based on the change in the sdpBindPwLocalStatusBits appropriate configuration changes may be required.

70.38 sdpBindPwPeerFaultAddrChanged

Table 1298: sdpBindPwPeerFaultAddrChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2315
Event name	sdpBindPwPeerFaultAddrChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.16

Property name	Value
Default severity	minor
Message format string	Status of SDP Bind *$sdpBindId$* in service *$svcId$* (customer *$cust Id$*) peer PW status IP address changed to *$sdpBindPwFaultInet Address$*
Cause	There was a change in the IP address included in the PW status message sent by the peer. This event is only generated if the IP address is the only information in the status message that changed. If the status bits changed as well, then the sdpBindPwPeerStatusBits Changed event will be generated instead.
Effect	N/A
Recovery	N/A

70.39 sdpBindPwPeerStatusBitsChanged

Table 1299: sdpBindPwPeerStatusBitsChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2313
Event name	sdpBindPwPeerStatusBitsChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.14
Default severity	minor
Message format string	Status of SDP Bind *$sdpBindId$* in service *$svcId$* (customer *$custId $*) peer PW status bits changed to *$sdpBindPwPeerStatusBitsString$*
Cause	There was a change in the PW status bits received from the peer.
Effect	N/A
Recovery	N/A

70.40 sdpBindReceivedProtSrcMac

Table 1300: sdpBindReceivedProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2325
Event name	sdpBindReceivedProtSrcMac
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.30
Default severity	minor
Message format string	Protected MAC *$protectedMacForNotify$* received on SDP Bind *$sdp BindId$* in service *$svcId$*.
Cause	The sdpBindReceivedProtSrcMac notification is generated when a protected source MAC is received on a TLS SDP-BIND with sdpBind TlsRestProtSrcMac 'true', or if the TLS SDP-BIND belongs to an SHG with tlsShgRestProtSrcMac set to 'true'.
Effect	If the sdpBindTlsRestProtSrcMacAction is set to 'discardFrame', the frame will be discarded.
Recovery	No action is required.

70.41 sdpBindSdpStateChangeProcessed

Table 1301: sdpBindSdpStateChangeProcessed properties

Property name	Value
Application name	SVCMGR
Event ID	2316
Event name	sdpBindSdpStateChangeProcessed
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.20
Default severity	major
Message format string	Processing of a SDP state change event is finished and the status of all affected SDP Bindings on SDP *$sdpNotifySdpId$* has been updated.
Cause	The processing of all SDP Bindings affected by a SDP state change event has finished.

Property name	Value
Effect	When a SDP changes state, all SDP Bindings associated with that SDP also change state. The sdpBindStatusChanged events are suppressed and when the processing of state changes for all SAPs associated with the port is finished, a single sdpBindSdpStateChange Processed event is generated.
Recovery	N/A

70.42 sdpBindStatusChanged

Table 1302: sdpBindStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2306
Event name	sdpBindStatusChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.6
Default severity	minor
Message format string	Status of SDP Bind *$sdpBindId$* in service *$svcId$* (customer *$cust Id$*) changed to admin= *$sdpBindAdminStatus$* oper=*$sdpBindOper Status$* flags=*$sdpBindOperFlags$*
Cause	There was a change in the administrative or operating status of an SDP Binding. This event is not generated whenever the SDP Binding operating status change is caused by an operating status change on the associated SDP.
Effect	N/A
Recovery	N/A

70.43 sdpBindTlsMacMoveExceeded

Table 1303: sdpBindTlsMacMoveExceeded properties

Property name	Value
Application name	SVCMGR
Event ID	2314

Property name	Value
Event name	sdpBindTlsMacMoveExceeded
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.15
Default severity	minor
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sdpBindNotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* and will retry in *$sdpBindTlsMacMoveNextUpTime$* seconds (retries left= *$sdpBindTlsMacMoveRateExcdLeft$* admin=*$sdpBindAdminStatus$* oper= *$sdpBindOperStatus$*) - detected on SDP Bind *$sdpBindId$*
Cause	This notification is generated when the TLS svcTlsMacMoveMaxRate has been exceeded for the SDP Bind.
Effect	The interface will be brought down and then brought back up automatically in sdpBindTlsMacMoveNextUpTime seconds if retries are remaining as indicated by sdpBindTlsMacMoveRateExcdLeft.
Recovery	If there are retries remaining, as indicated by sdpBindTlsMacMoveRateExcdLeft, the interface will be brought back up automatically in sdpBindTlsMacMoveNextUpTime seconds. If no retries are remaining, the interface must be manually brought back up by an adminstrator.

70.44 sdpBindTlsMacMoveExceedNonBlock

Table 1304: sdpBindTlsMacMoveExceedNonBlock properties

Property name	Value
Application name	SVCMGR
Event ID	2327
Event name	sdpBindTlsMacMoveExceedNonBlock
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.32
Default severity	minor
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sdpBindNotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* - detected on SDP Bind *$sdpBindId$*
Cause	The sdpBindTlsMacMoveExceedNonBlock notification is generated when the SDP exceeds the TLS svcTlsMacMoveMaxRate even when sdpBindTlsLimitMacMove is set to 'nonBlocking'.In case of Provider Backbone Bridging (PBB), if the MAC address that exceeds the rate is in ISID-VPLS(iVpls) FDB and sdp binding that detects the move is in

Property name	Value
	Backbone-VPLS(bVpls), the notification will be generated with svcId, custId of I-VPLS and B-VPLS sdpBindId.
Effect	This notification is informational only.
Recovery	User can adjust the value of svcTlsMacMoveMaxRate to reduce the frequency of this notification."

70.45 sdpControlPwActiveStateChg

Table 1305: sdpControlPwActiveStateChg properties

Property name	Value
Application name	SVCMGR
Event ID	2345
Event name	sdpControlPwActiveStateChg
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.36
Default severity	minor
Message format string	Control PW Active status is *$sdpControlPWIsActive$* on SDP:*$sdpId$*
Cause	The sdpControlPwActiveStateChg notification is generated when when the SDP control PW Active value changes on that SDP.
Effect	Control pseudo-wire state change could affect related SDP bindings.
Recovery	A change in the configuration may be required.

70.46 sdpEgrIfsNetDomInconsCntChanged

Table 1306: sdpEgrIfsNetDomInconsCntChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2323
Event name	sdpEgrIfsNetDomInconsCntChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.28

Property name	Value
Default severity	major
Message format string	The system at present has *$sdpEgIfNetDomainInconsCount$* SDPs that can use network interfaces which are not associated with the respective SDP's network domain.
Cause	The system at present has zero or more SDPs that can use network interfaces which are not associated with the respective SDP's network domain.
Effect	N/A
Recovery	N/A

70.47 sdpKeepAliveLateReply

Table 1307: sdpKeepAliveLateReply properties

Property name	Value
Application name	SVCMGR
Event ID	2310
Event name	sdpKeepAliveLateReply
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	SDP *$sdpId$* probe *$probeSeqNumber$* response comes after timeout
Cause	A SDP keep alive session received a late reply.
Effect	N/A
Recovery	N/A

70.48 sdpKeepAliveProbeFailure

Table 1308: sdpKeepAliveProbeFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2309

Property name	Value
Event name	sdpKeepAliveProbeFailure
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	SDP *$sdpId$*: failed with error: *$Error$*
Cause	A sdp keep alive probe has not responded correctly.
Effect	N/A
Recovery	N/A

70.49 sdpKeepAliveStarted

Table 1309: sdpKeepAliveStarted properties

Property name	Value
Application name	SVCMGR
Event ID	2307
Event name	sdpKeepAliveStarted
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	SDP *$sdpId$* keepalive has started
Cause	A sdp keep alive was started.
Effect	N/A
Recovery	N/A

70.50 sdpKeepAliveStopped

Table 1310: sdpKeepAliveStopped properties

Property name	Value
Application name	SVCMGR
Event ID	2308

Property name	Value
Event name	sdpKeepAliveStopped
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	SDP *$sdpId$* keepalive has stopped
Cause	A sdp keep alive was stopped.
Effect	N/A
Recovery	N/A

70.51 sdpPbbActvPwWithNonActvCtrlPwChg

Table 1311: sdpPbbActvPwWithNonActvCtrlPwChg properties

Property name	Value
Application name	SVCMGR
Event ID	2330
Event name	sdpPbbActvPwWithNonActvCtrlPwChg
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.35
Default severity	minor
Message format string	First/last PW is active/standby/down (*$sdpPbbActvPwWithNonActvCtrlPw$*) on the BEB where control PW is standby/down on SDP: *$sdpId$*
Cause	The sdpPbbActvPwWithNonActvCtrlPwChg notification is generated when last pseudo-wire (PW) goes standby or down and when first PW becomes active on the Backbone Edge Bridge (BEB) where control PW is standby or down on that SDP.
Effect	There is a change which caused last active PW to become standby or down and when first PW becomes active.
Recovery	sdpPbbActvPwWithNonActvCtrlPwChg event with sdpPbbActvPwWithNonActvCtrlPw set to 'false' indicate clearing of sdpPbbActvPwWithNonActvCtrlPwChg with sdpPbbActvPwWithNonActvCtrlPw set to 'true'."

70.52 sdpStatusChanged

Table 1312: sdpStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2303
Event name	sdpStatusChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.3
Default severity	minor
Message format string	Status of SDP *$sdpId$* changed to admin=*$sdpAdminStatus$* oper=*$sdpOperStatus$*
Cause	There was a change in the administrative or operating status of an SDP.
Effect	N/A
Recovery	N/A

70.53 sdpTlsMacAddrLimitAlarmCleared

Table 1313: sdpTlsMacAddrLimitAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2312
Event name	sdpTlsMacAddrLimitAlarmCleared
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.8
Default severity	minor
Message format string	Number of MAC addr learned by this spoke sdp bind *$sdpBindId$* in service *$svcId$* dropped below the LowWaterMark.
Cause	The number of MAC addresses stored in the FDB for a spoke sdp-bind dropped below the low watermark.
Effect	N/A
Recovery	N/A

70.54 sdpTlsMacAddrLimitAlarmRaised

Table 1314: sdpTlsMacAddrLimitAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2311
Event name	sdpTlsMacAddrLimitAlarmRaised
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.7
Default severity	minor
Message format string	Number of MAC addr learned by spoke sdp bind *$sdpBindId$* in service *$svcId$* reached the HighWaterMark.
Cause	The number of MAC addresses stored in the FDB for a spoke sdp-bind exceeded the high watermark.
Effect	N/A
Recovery	N/A

70.55 svcArpHostOverride

Table 1315: svcArpHostOverride properties

Property name	Value
Application name	SVCMGR
Event ID	2091
Event name	svcArpHostOverride
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.77
Default severity	minor
Message format string	Existing ARP host (ipAddr = *$svcArpHostIpAddr$*, macAddr = *$svc NotifyMacAddress$*) in service *$svcId$* overridden to (ipAddr = *$svcArp HostIpAddr$*, macAddr = *$svcArpHostMacAddr$*)
Cause	The system overrides the MAC address of an ARP host, because an ARP host with the same IP address as a known ARP host has appeared with a different MAC address.

Property name	Value
Effect	The MAC address of the known ARP host has changed.
Recovery	No recovery required.

70.56 svcArpHostPopulateErr

Table 1316: svcArpHostPopulateErr properties

Property name	Value
Application name	SVCMGR
Event ID	2520
Event name	svcArpHostPopulateErr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.27
Default severity	warning
Message format string	ARP host table population error on SAP *$sapEncapValue$* in service *$svcId$* - *$svcArpHostPopulateError$*
Cause	ARP Host populate is enabled and upon the reception of an ARP message, an ARP host could not be instantiated. The failure reason is specified in the svcArpHostPopulateError.
Effect	The ARP host was not instantiated. The source of the ARP message was not allowed access to the network service.
Recovery	The recovery action depends on the failure reason.

70.57 svcBgpEvpnDupMacAddrsCleared

Table 1317: svcBgpEvpnDupMacAddrsCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2332
Event name	svcBgpEvpnDupMacAddrsCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.43
Default severity	minor

Property name	Value
Message format string	VPLS Service $svcId no longer has MAC(s) detected as duplicates by EVPN mac-duplication detection.
Cause	The svcBgpEvpnDupMacAddrsCleared notification is generated when no more MAC addresses are detected as duplicate in a VPLS EVPN context.
Effect	No MAC addresses are detected as duplicate.
Recovery	None needed.

70.58 svcBgpEvpnDupMacAddrsDetected

Table 1318: svcBgpEvpnDupMacAddrsDetected properties

Property name	Value
Application name	SVCMGR
Event ID	2331
Event name	svcBgpEvpnDupMacAddrsDetected
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.42
Default severity	minor
Message format string	VPLS Service $svcId has MAC(s) detected as duplicates by EVPN mac-duplication detection.
Cause	The svcBgpEvpnDupMacAddrsDetected notification is generated when at least one MAC address is detected as duplicate in a VPLS EVPN context.
Effect	At least one MAC address is detected as duplicate.
Recovery	None needed.

70.59 svcBindSysHiUsageAlarmCleared

Table 1319: svcBindSysHiUsageAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2342

Property name	Value
Event name	svcBindSysHiUsageAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.53
Default severity	minor
Message format string	The number of VXLAN bindings in the system is below 90% of the system VXLAN bindings limit.
Cause	The svcBindSysHiUsageAlarmCleared notification is generated when the number of VXLAN binds drops below 90% of the system VXLAN bind limit.
Effect	90% of the system VXLAN bind limit is reached.
Recovery	None needed.

70.60 svcBindSysHiUsageAlarmRaised

Table 1320: svcBindSysHiUsageAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2341
Event name	svcBindSysHiUsageAlarmRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.52
Default severity	minor
Message format string	The number of VXLAN bindings in the system exceeds 95% of the system VXLAN bindings limit.
Cause	The svcBindSysHiUsageAlarmRaised notification is generated when the number of VXLAN binds exceeds 95% of the system VXLAN bind limit.
Effect	95% of the system VXLAN bind limit is reached.
Recovery	None needed.

70.61 svcEndPointMacLimitAlarmCleared

Table 1321: svcEndPointMacLimitAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2508
Event name	svcEndPointMacLimitAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.19
Default severity	minor
Message format string	Number of MAC addr learned by endpoint " *$endPointName$*" in service *$svcId$* reached the LowWaterMark.
Cause	The number of MAC addresses stored in the FDB for an endpoint dropped below the low watermark. This event also takes into consideration the static MAC addresses configured on the endpoint and learned MAC addresses in all spokes associated with the endpoint."
Effect	N/A
Recovery	N/A

70.62 svcEndPointMacLimitAlarmRaised

Table 1322: svcEndPointMacLimitAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2507
Event name	svcEndPointMacLimitAlarmRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.18
Default severity	minor
Message format string	Number of MAC addr learned by endpoint " *$endPointName$*" in service *$svcId$* reached the HighWaterMark.
Cause	The number of MAC addresses stored in the FDB for a endpoint exceeded the high watermark. This event also takes into consideration

Property name	Value
	the static MAC addresses configured on the endpoint and learned MAC addresses in all spokes associated with the endpoint.
Effect	N/A
Recovery	N/A

70.63 svcEpipePbbOperStatusChanged

Table 1323: svcEpipePbbOperStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2128
Event name	svcEpipePbbOperStatusChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.28
Default severity	minor
Message format string	Operational Status of PBB Tunnel with E-pipe service *$svcId$* changed to *$svcEpipePbbOperState$*.
Cause	There was a change in the operating status of the PBB tunnel associated with an E-pipe service.
Effect	N/A
Recovery	N/A

70.64 svcEPMCEPConfigMismatch

Table 1324: svcEPMCEPConfigMismatch properties

Property name	Value
Application name	SVCMGR
Event ID	2522
Event name	svcEPMCEPConfigMismatch
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.29

Property name	Value
Default severity	warning
Message format string	Multi-chassis endpoint *$svcEndPointMCEPId$* associated with endpoint "*$svcEndPointName$*" in service *$svcId$* detected a mismatch in the config of multi-chassis endpoint peer.
Cause	A service multi-chassis endpoint detected a mismatch in the configuration of the multi-chassis endpoint peer.
Effect	N/A
Recovery	N/A

70.65 svcEPMCEPConfigMismatchResolved

Table 1325: svcEPMCEPConfigMismatchResolved properties

Property name	Value
Application name	SVCMGR
Event ID	2523
Event name	svcEPMCEPConfigMismatchResolved
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.30
Default severity	warning
Message format string	Multi-chassis endpoint *$svcEndPointMCEPId$* associated with endpoint "*$svcEndPointName$*" in service *$svcId$* resolved a mismatch in the config of multi-chassis endpoint peer.
Cause	A multi-chassis endpoint resolved the mismatch in the configuration of a multi-chassis endpoint peer.
Effect	N/A
Recovery	N/A

70.66 svcEPMCEPPassiveModeActive

Table 1326: svcEPMCEPPassiveModeActive properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2524
Event name	svcEPMCEPPassiveModeActive
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.31
Default severity	warning
Message format string	Multi-chassis endpoint *$svcEndPointMCEPId$* associated with endpoint "*$svcEndPointName$*" in service *$svcId$* in passive-mode became active
Cause	A multi-chassis endpoint on a multi-chassis peer in passive-mode (of multi-chassis peer) became passive-mode active by detecting more than one active spoke-sdp in the multi-chassis endpoint with 'pwFwding Standby' bit cleared per sdpBindPwPeerStatusBits object.
Effect	N/A
Recovery	N/A

70.67 svcEPMCEPPassiveModePassive

Table 1327: svcEPMCEPPassiveModePassive properties

Property name	Value
Application name	SVCMGR
Event ID	2525
Event name	svcEPMCEPPassiveModePassive
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.32
Default severity	warning
Message format string	Multi-chassis endpoint *$svcEndPointMCEPId$* associated with endpoint "*$svcEndPointName$*" in service *$svcId$* in passive-mode became passive
Cause	A multi-chassis endpoint on a multi-chassis peer in passive-mode (of multi-chassis peer) became passive-mode active by detecting at most one active spoke-sdp in the multi-chassis endpoint with 'pwFwding Standby' bit set per sdpBindPwPeerStatusBits object.
Effect	N/A
Recovery	N/A

70.68 svcEvpnDestSysHiUsgClr

Table 1328: svcEvpnDestSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2093
Event name	svcEvpnDestSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.79
Default severity	minor
Message format string	The number of EVPN destinations(MPLS and VXLAN) in the system is below 90% of the system limit
Cause	The svcEvpnDestSysHiUsgClr notification is generated when the number of EVPN destinations(MPLS and VXLAN) in the system drops below 90% of the system limit.
Effect	The system EVPN destinations(MPLS and VXLAN) limit drops below 90%.
Recovery	None needed.

70.69 svcEvpnDestSysHiUsgSet

Table 1329: svcEvpnDestSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2092
Event name	svcEvpnDestSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.78
Default severity	minor
Message format string	The number of EVPN destinations(MPLS and VXLAN) in the system exceeds 95% of the system limit
Cause	The svcEvpnDestSysHiUsgSet notification is generated when the number of EVPN destinations(MPLS and VXLAN) in the system exceeds 95% of the system limit.

Property name	Value
Effect	95% of the system EVPN destinations(MPLS and VXLAN) limit is reached.
Recovery	None needed.

70.70 svcEvpnMHEsEviDFStateChgd

Table 1330: svcEvpnMHEsEviDFStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2094
Event name	svcEvpnMHEsEviDFStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.80
Default severity	minor
Message format string	Ethernet Segment: *$tmnxSvcSysEthSegName$*, EVI:*$svcEvpnMHEthSegEvi$*, Designated Forwarding state changed to: *$svcEvpnMHEthSegEviIsDF$*
Cause	The svcEvpnMHEsEviDFStateChgd notification is generated when there is a change in the ethernet segment EVI designated forwarder state.
Effect	The forwarding state of the ethernet segment evi is changed.
Recovery	None needed.

70.71 svcEvpnMHEsIsidDFStateChgd

Table 1331: svcEvpnMHEsIsidDFStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2095
Event name	svcEvpnMHEsIsidDFStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.81

Property name	Value
Default severity	minor
Message format string	Ethernet Segment: *$tmnxSvcSysEthSegName$*, ISID:*$svcEvpnMHEthSegIsid$*, Designated Forwarding state changed to: *$svcEvpnMHEthSegIsidIsDF$*
Cause	The svcEvpnMHEsIsidDFStateChgd notification is generated when there is a change in the ethernet segment ISID designated forwarder state.
Effect	The forwarding state of the ethernet segment isid is changed.
Recovery	None needed.

70.72 svcEvpnMplsMacMoveExceedNonBlock

Table 1332: svcEvpnMplsMacMoveExceedNonBlock properties

Property name	Value
Application name	SVCMGR
Event ID	2068
Event name	svcEvpnMplsMacMoveExceedNonBlock
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.60
Default severity	minor
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sapTlsNotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* - detected on *$tlsFdbBackboneDstMac$*
Cause	The svcEvpnMplsMacMoveExceedNonBlock notification is generated when the EVPN MPLS destination exceeds the TLS svcTlsMacMoveMaxRate when sapTlsLimitMacMove is set to 'nonBlocking'.
Effect	This notification is informational only.
Recovery	User can adjust the value of svcTlsMacMoveMaxRate to reduce the frequency of this notification.

70.73 svcEvpnMplsTEPEgrBndSvcHiUsgClr

Table 1333: svcEvpnMplsTEPEgrBndSvcHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2357
Event name	svcEvpnMplsTEPEgrBndSvcHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.67
Default severity	minor
Message format string	Service *$svcId$* has EVPN MPLS tunnel endpoint-egress multicast binds below 90% of the per-service limit
Cause	The svcEvpnMplsTEPEgrBndSvcHiUsgClr notification is generated when the number of EVPN MPLS tunnel endpoint-egress multicast binds in a VPLS service drops below 90% of the per-service limit.
Effect	The VPLS service has reached 90% of the EVPN MPLS tunnel endpoint-egress multicast bind multicast limit.
Recovery	None needed.

70.74 svcEvpnMplsTEPEgrBndSvcHiUsgSet

Table 1334: svcEvpnMplsTEPEgrBndSvcHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2356
Event name	svcEvpnMplsTEPEgrBndSvcHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.66
Default severity	minor
Message format string	Service *$svcId$* has EVPN MPLS tunnel endpoint-egress multicast binds in excess of 95% of the per-service limit
Cause	The svcEvpnMplsTEPEgrBndSvcHiUsgSet notification is generated when the number of EVPN MPLS tunnel endpoint-egress multicast binds in a VPLS service exceeds 95% of the per-service limit.

Property name	Value
Effect	The VPLS service has reached 95% of the EVPN MPLS tunnel endpoint-egress multicast bind multicast limit.
Recovery	None needed.

70.75 svcEvpnMplsTEPEgrBndSysHiUsgClr

Table 1335: svcEvpnMplsTEPEgrBndSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2355
Event name	svcEvpnMplsTEPEgrBndSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.65
Default severity	minor
Message format string	The number of EVPN MPLS tunnel endpoint-egress binds in the system is below 90% of the system limit
Cause	The svcEvpnMplsTEPEgrBndSysHiUsgClr notification is generated when the number of EVPN MPLS tunnel endpoint-egress binds in the system drops below 90% of the system limit.
Effect	90% of the system EVPN MPLS tunnel endpoint-egress bind limit is reached.
Recovery	None needed.

70.76 svcEvpnMplsTEPEgrBndSysHiUsgSet

Table 1336: svcEvpnMplsTEPEgrBndSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2354
Event name	svcEvpnMplsTEPEgrBndSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.64

Property name	Value
Default severity	minor
Message format string	The number of EVPN MPLS tunnel endpoint-egress binds in the system exceeds 95% of the system limit
Cause	The svcEvpnMplsTEPEgrBndSysHiUsgSet notification is generated when the number of EVPN MPLS tunnel endpoint-egress multicast binds in the system exceeds 95% of the system limit.
Effect	95% of the system EVPN MPLS tunnel endpoint-egress multicast bind limit is reached.
Recovery	None needed.

70.77 svcEvpnMplsTEPHiUsageCleared

Table 1337: svcEvpnMplsTEPHiUsageCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2353
Event name	svcEvpnMplsTEPHiUsageCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.63
Default severity	minor
Message format string	The number of EVPN MPLS tunnel endpoints in the system is below 90% of the system limit
Cause	The svcEvpnMplsTEPHiUsageCleared notification is generated when the number of EVPN MPLS tunnel endpoints in the system drops below 90% of system limit.
Effect	90% of the system EVPN MPLS tunnel endpoint limit is reached.
Recovery	None needed.

70.78 svcEvpnMplsTEPHiUsageRaised

Table 1338: svcEvpnMplsTEPHiUsageRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2352
Event name	svcEvpnMplsTEPHiUsageRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.62
Default severity	minor
Message format string	The number of EVPN MPLS tunnel endpoints in the system exceeds 95% of the system limit.
Cause	The svcEvpnMplsTEPHiUsageRaised notification is generated when the number of EVPN MPLS tunnel endpoints in the system exceeds 95% of the system limit.
Effect	95% of the system EVPN MPLS tunnel endpoint limit is reached.
Recovery	None needed.

70.79 svcEvpnRcvdProtSrcMac

Table 1339: svcEvpnRcvdProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2096
Event name	svcEvpnRcvdProtSrcMac
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.82
Default severity	minor
Message format string	Protected Mac *$protectedMacForNotify$* received over EVPN in service *$svcId$*.
Cause	The svcEvpnRcvdProtSrcMac notification is generated when a protected source MAC is received.
Effect	The frame is discarded.
Recovery	None needed.

70.80 svcFdbMimDestTblFullAlrm

Table 1340: svcFdbMimDestTblFullAlrm properties

Property name	Value
Application name	SVCMGR
Event ID	2515
Event name	svcFdbMimDestTblFullAlrm
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.21
Default severity	minor
Message format string	System limit of PBB Backbone MAC Address indices *$svcTotalFdbMimDestIdxEntries$* is reached
Cause	The system limit of Backbone MAC address indices was reached.
Effect	Further events are not generated as long as the value of svcTotalFdbMimDestIdxEntries object remains under 10 percent of the limit.
Recovery	N/A

70.81 svcFdbMimDestTblFullAlrmCleared

Table 1341: svcFdbMimDestTblFullAlrmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2516
Event name	svcFdbMimDestTblFullAlrmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.22
Default severity	minor
Message format string	Number of PBB Backbone MAC Address indices *$svcTotalFdbMimDestIdxEntries$* is now at 95 percent of system limit
Cause	The number of PBB backbone MAC address indices has fallen to 95 percent of the system limit after hitting the system limit.
Effect	N/A

Property name	Value
Recovery	N/A

70.82 svcMacFdbTblFullAlarm

Table 1342: svcMacFdbTblFullAlarm properties

Property name	Value
Application name	SVCMGR
Event ID	2537
Event name	svcMacFdbTblFullAlarm
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.36
Default severity	minor
Message format string	System limit of FDB MAC Address table *$svcMacFdbRecords$* is reached
Cause	The svcMacFdbTblFullAlarm notification is raised when system limit of FDB records is reached. Further traps are not generated as long as the value of svcMacFdbRecords object remains under 5 percent of the limit. The system limit of Backbone MAC address indices was reached.
Effect	System will not be able to add new MAC addresses to the FDB table.
Recovery	Optimize the MAC FDB addresses assigned to different services.

70.83 svcMacFdbTblFullAlarmCleared

Table 1343: svcMacFdbTblFullAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2538
Event name	svcMacFdbTblFullAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.37
Default severity	minor

Property name	Value
Message format string	Number of FDB MAC Address table *$svcMacFdbRecords$* is now at 95 percent of system limit
Cause	The svcMacFdbTblFullAlarmCleared notification is raised when number of FDB records used reaches under 95 percent of the system limit after svcMacFdbTblFullAlarm notification had been raised.
Effect	N/A
Recovery	None.

70.84 svcMSPwRetryExpiredNotif

Table 1344: svcMSPwRetryExpiredNotif properties

Property name	Value
Application name	SVCMGR
Event ID	2544
Event name	svcMSPwRetryExpiredNotif
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.40
Default severity	minor
Message format string	Retry timer *$svcMSPwPeRetryExpired$* for spoke-sdp-fec: *$svcMSPwPeId$* in service: *$svcId$*
Cause	The svcMSPwRetryExpiredNotif notification is raised when retry-timer expires for this multi-segment pseudo-wire provider-edge (svcMSPwPeId) in the service.
Effect	There will be no more retries to establish connection from this svcMSPwPeId.
Recovery	svcMSPwPeId may need to be shutdown and may need to restart the retries."

70.85 svcMSPwRtMisconfig

Table 1345: svcMSPwRtMisconfig properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2541
Event name	svcMSPwRtMisconfig
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.38
Default severity	minor
Message format string	Misconfigured multi-segment pseudo-wire SAII= *$svcMSPwPeSaiiGlobalId$*:*$svcMSPwPeSaiiPrefix$*:*$svcMSPwPeSaiiAcId$* TAII= *$svcMSPwPeTaiiGlobalId$*:*$svcMSPwPeTaiiPrefix$*:*$svcMSPwPeTaiiAcId$*
Cause	The svcMSPwRtMisconfig notification is raised when there is mis-configuration discovered between two signalling multi-segment pseudo-wires. The following mis-configuration would cause this notification: - Both multi-segment pseudo-wires are configured to be master
Effect	Communication between the multi-segment pseudo-wires will fail.
Recovery	Mis-configuration between the two multi-segment pseudo-wire needs to be corrected.

70.86 svcOperGrpOperStatusChanged

Table 1346: svcOperGrpOperStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2542
Event name	svcOperGrpOperStatusChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.39
Default severity	minor
Message format string	Oper-group *$svcOperGrpName$* changed status to *$svcOperGrpOperStatus$*
Cause	The svcOperGrpOperStatusChanged notification is generated when there is a change in the value of svcOperGrpOperStatus.
Effect	Status of the one or more of the members of the operational group has changed.
Recovery	Operational status of the members of the operational-group will need to be investigated.

70.87 svcPersistencyProblem

Table 1347: svcPersistencyProblem properties

Property name	Value
Application name	SVCMGR
Event ID	2517
Event name	svcPersistencyProblem
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.24
Default severity	warning
Message format string	Persistency problem in service *$svcId$*: *$tmnxFailureDescription$*
Cause	A persistency problems occurred.
Effect	N/A
Recovery	N/A

70.88 svcRestoreHostProblem

Table 1348: svcRestoreHostProblem properties

Property name	Value
Application name	SVCMGR
Event ID	2528
Event name	svcRestoreHostProblem
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.33
Default severity	warning
Message format string	Problem occured while processing host persistency record (Addr = *$svcHostAddr$*) - *$tmnxFailureDescription$*
Cause	N/A
Effect	N/A
Recovery	N/A

70.89 svcSiteMinDnTimerStateChg

Table 1349: svcSiteMinDnTimerStateChg properties

Property name	Value
Application name	SVCMGR
Event ID	2366
Event name	svcSiteMinDnTimerStateChg
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.76
Default severity	warning
Message format string	Service:*$svcId$* site: *$svcNotifSiteName$* min-down-timer state changed to:*$svcNotifSiteMinDnTimerState$* with timer: *$svcNotifSiteMinDnTimer$* secs and timer-remaining:*$svcNotifSiteMinDnTimerRemain$* secs
Cause	The svcSiteMinDnTimerStateChg notification is generated when site specific minimum-down-timer starts/canceled/extended/expires.
Effect	svcSiteMinDnTimerState indicate the new state of the site minimum-down-timer.
Recovery	None needed.

70.90 svcStatusChanged

Table 1350: svcStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2103
Event name	svcStatusChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.3
Default severity	minor
Message format string	Status of service *$svcId$* (customer *$custId$*) changed to administrative state: *$svcAdminStatus$*, operational state: *$svcOperStatus$*
Cause	There was a change in the administrative or operating status of a service.

Property name	Value
Effect	N/A
Recovery	N/A

70.91 svcSysEvpnESDfPrefOperValChange

Table 1351: svcSysEvpnESDfPrefOperValChange properties

Property name	Value
Application name	SVCMGR
Event ID	2106
Event name	svcSysEvpnESDfPrefOperValChange
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.89
Default severity	minor
Message format string	Ethernet Segment: *$tmnxSvcSysEthSegName$*, The Oper DF preference value changed to *$svcSysEvpnESDfPrefElecOperValue $* and/or the DP value changed to *$svcSysEvpnESDfPrefElecDnt Preempt$*.
Cause	The svcSysEvpnESDfPrefOperValChange notification is generated when the ES route is first advertised or when the Oper preference and/or DP value changes.
Effect	None.
Recovery	None needed.

70.92 svcTlsDupVTEPEgrVNICleared

Table 1352: svcTlsDupVTEPEgrVNICleared properties

Property name	Value
Application name	SVCMGR
Event ID	2334
Event name	svcTlsDupVTEPEgrVNICleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.45

Property name	Value
Default severity	minor
Message format string	VTEP *$svcVTEPEgrVNIVTEPAddress$*, Egress VNI *$svcVTEPEgrVNIEgrVNI$* no longer used in more than one service.
Cause	The svcTlsDupVTEPEgrVNICleared notification is generated when a previously duplicate VTEP-Egress VNI is no longer used in more than one service in the system.
Effect	The VTEP-Egress VNI is no longer duplicate.
Recovery	None needed.

70.93 svcTlsDupVTEPEgrVNIDetected

Table 1353: svcTlsDupVTEPEgrVNIDetected properties

Property name	Value
Application name	SVCMGR
Event ID	2333
Event name	svcTlsDupVTEPEgrVNIDetected
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.44
Default severity	minor
Message format string	Attempt to use VTEP *$svcVTEPEgrVNIVTEPAddress$*, Egress VNI *$svcVTEPEgrVNIEgrVNI$* in more than one service.
Cause	The svcTlsDupVTEPEgrVNIDetected notification is generated when a duplicate VTEP-Egress VNI is detected in the system.
Effect	A VTEP-Egress VNI is detected as duplicate.
Recovery	None needed.

70.94 svcTlsEvpnTunnNHopHiUsgAlarmClr

Table 1354: svcTlsEvpnTunnNHopHiUsgAlarmClr properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2351
Event name	svcTlsEvpnTunnNHopHiUsgAlarmClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.61
Default severity	minor
Message format string	Dropped below 90% of EVPN tunnel interface IP next-hop limit for service *$svcId$*
Cause	The svcTlsEvpnTunnNHopHiUsgAlarmClr notification is generated when the number of EVPN tunnels next-hop in the service drops to 90% of the limit.
Effect	Dropped below 90% of EVPN tunnel interface IP next-hop limit for service.
Recovery	None needed.

70.95 svcTlsEvpnTunnNHopHiUsgAlarmSet

Table 1355: svcTlsEvpnTunnNHopHiUsgAlarmSet properties

Property name	Value
Application name	SVCMGR
Event ID	2350
Event name	svcTlsEvpnTunnNHopHiUsgAlarmSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.60
Default severity	minor
Message format string	Reached 95% of EVPN tunnel interface IP next-hop limit for service *$svcId$*
Cause	The svcTlsEvpnTunnNHopHiUsgAlarmSet notification is generated when the number of EVPN tunnels next-hops in the service exceeds 95% of the limit.
Effect	Reached 95% of the EVPN tunnel interface IP next-hop limit for service.
Recovery	Verify the BGP-EVPN configuration to see if configuration changes are needed to reduce this."

70.96 svcTlsFdbTableFullAlarmCleared

Table 1356: svcTlsFdbTableFullAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2105
Event name	svcTlsFdbTableFullAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.5
Default severity	minor
Message format string	FDB table utilization of service *$svcId$* (customer *$custId$*) crossed its low watermark
Cause	The utilization of the FDB table has gone below its low watermark value.
Effect	N/A
Recovery	N/A

70.97 svcTlsFdbTableFullAlarmRaised

Table 1357: svcTlsFdbTableFullAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2104
Event name	svcTlsFdbTableFullAlarmRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.4
Default severity	minor
Message format string	FDB table utilization of service *$svcId$* (customer *$custId$*) crossed its high watermark
Cause	The utilization of the FDB table is above its high watermark."
Effect	N/A
Recovery	N/A

70.98 svcTlsGroupOperStatusChanged

Table 1358: svcTlsGroupOperStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2533
Event name	svcTlsGroupOperStatusChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.35
Default severity	minor
Message format string	Service *$svcId$* VPLS group *$svcTlsGroupId$* changed status to *$svcTlsGroupOperStatus$* with last-error: *$svcTlsGroupLastError$*
Cause	Service VPLS Group status changed
Effect	N/A
Recovery	N/A

70.99 svcTlsMacPinningViolation

Table 1359: svcTlsMacPinningViolation properties

Property name	Value
Application name	SVCMGR
Event ID	2011
Event name	svcTlsMacPinningViolation
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.11
Default severity	warning
Message format string	Relearn attempt on *$macPinningViolatingRowDescr$* in service *$svcId $* for mac address *$macPinningMacAddress$* pinned on *$macPinningPinnedRowDescr$*
Cause	An attempt was made to assign a MAC address to another interface while this MAC address is pinned (i.e. assigned fixed to an interface).
Effect	The query will be ignored

Property name	Value
Recovery	No recovery is necessary.

70.100 svcTlsMfibTableFullAlarmCleared

Table 1360: svcTlsMfibTableFullAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2402
Event name	svcTlsMfibTableFullAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.10
Default severity	minor
Message format string	MFIB table utilization of service *$svcId$* (customer *$custId$*) crossed its low watermark
Cause	The utilization of the MFIB table has dropped below the low watermark.
Effect	N/A
Recovery	N/A

70.101 svcTlsMfibTableFullAlarmRaised

Table 1361: svcTlsMfibTableFullAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2401
Event name	svcTlsMfibTableFullAlarmRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.9
Default severity	minor
Message format string	MFIB table utilization of service *$svcId$* (customer *$custId$*) crossed its high watermark
Cause	The utilization of the MFIB table rose above the high watermark.

Property name	Value
Effect	N/A
Recovery	N/A

70.102 svcTlsMrpAttrRegistrationFailed

Table 1362: svcTlsMrpAttrRegistrationFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2120
Event name	svcTlsMrpAttrRegistrationFailed
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.20
Default severity	minor
Message format string	An MRP attribute with type= *$svcTlsMrpAttrType$* value=$svcTlsMrp AttrValue failed to register in service *$svcId$* (customer *$custId$*) due to: *$svcTlsMrpAttrRegFailedReason$*
Cause	An MRP attributed failed to register in a service.
Effect	N/A
Recovery	N/A

70.103 svcTlsMrpAttrTblFullAlarmCleared

Table 1363: svcTlsMrpAttrTblFullAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2126
Event name	svcTlsMrpAttrTblFullAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.26
Default severity	minor

Property name	Value
Message format string	MRP attribute table utilization of service *$svcId$* (customer *$custId$*) crossed its low watermark
Cause	The utilization of the MRP attribute table fell below the low watermark.
Effect	N/A
Recovery	N/A

70.104 svcTlsMrpAttrTblFullAlarmRaised

Table 1364: svcTlsMrpAttrTblFullAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2125
Event name	svcTlsMrpAttrTblFullAlarmRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.25
Default severity	minor
Message format string	MRP attribute table utilization of service *$svcId$* (customer *$custId$*) crossed its high watermark
Cause	The utilization of the MRP attribute table rose above the high watermark.
Effect	N/A
Recovery	N/A

70.105 svcTlsProxyArpDupClear

Table 1365: svcTlsProxyArpDupClear properties

Property name	Value
Application name	SVCMGR
Event ID	2347
Event name	svcTlsProxyArpDupClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.57
Default severity	minor
Message format string	A duplicate proxy ARP entry *$svcTlsProxyArpIpAddr$* is cleared in service *$svcId$*
Cause	The svcTlsProxyArpDupDetect notification is generated when a duplicate ARP entry is cleared.
Effect	The proxy ARP entry is deleted or is overwritten by static entry.
Recovery	None needed.

70.106 svcTlsProxyArpDupDetect

Table 1366: svcTlsProxyArpDupDetect properties

Property name	Value
Application name	SVCMGR
Event ID	2346
Event name	svcTlsProxyArpDupDetect
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.56
Default severity	minor
Message format string	A duplicate proxy ARP entry was detected with new MAC *$svcNotif TlsProxyMacAddr$* for entry IP *$svcTlsProxyArpIpAddr$* MAC *$svcTls ProxyArpMacAddr$* in service *$svcId$*
Cause	The svcTlsProxyArpDupDetect notification is generated when duplicate detection criteria is met when a new mac address overwrites the existing mac address for the proxy arp entry.
Effect	A traffic disruption may occur if both IP addresses are active.
Recovery	Identify the systems using the old MAC address and correct the configuration."

70.107 svcTlsProxyArpSvcHiUsgClr

Table 1367: svcTlsProxyArpSvcHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2361
Event name	svcTlsProxyArpSvcHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.71
Default severity	minor
Message format string	Service *$svcId$* has proxy ARP entries below 90% of the per-service limit
Cause	The svcTlsProxyArpSvcHiUsgClr notification is generated when the number of proxy ARP entries in a VPLS service drops below 90% of the per-service limit.
Effect	The VPLS service has reached 90% of the proxy ARP entries limit.
Recovery	None needed.

70.108 svcTlsProxyArpSvcHiUsgSet

Table 1368: svcTlsProxyArpSvcHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2360
Event name	svcTlsProxyArpSvcHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.70
Default severity	minor
Message format string	Service *$svcId$* has proxy ARP entries in excess of 95% of the per-service limit
Cause	The svcTlsProxyArpSvcHiUsgSet notification is generated when the number of proxy ARP entries in a VPLS service exceeds 95% of the per-service limit.
Effect	The VPLS service has reached 95% of the proxy ARP entries limit.

Property name	Value
Recovery	None needed.

70.109 svcTlsProxyArpSysHiUsgClr

Table 1369: svcTlsProxyArpSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2359
Event name	svcTlsProxyArpSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.69
Default severity	minor
Message format string	The proxy ARP entries is below 90% of the system limit
Cause	The svcTlsProxyArpSysHiUsgClr notification is generated when the number of proxy ARP entries in the system drops below 90% of the system limit.
Effect	90% of the system proxy ARP entries limit is reached.
Recovery	None needed.

70.110 svcTlsProxyArpSysHiUsgSet

Table 1370: svcTlsProxyArpSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2358
Event name	svcTlsProxyArpSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.68
Default severity	minor
Message format string	The proxy ARP entries in the system exceeds 95% of the system limit

Property name	Value
Cause	The svcTlsProxyArpSysHiUsgSet notification is generated when the number of proxy ARP entries in the system exceeds 95% of the system limit.
Effect	95% of the system proxy ARP entries limit is reached.
Recovery	None needed.

70.111 svcTlsProxyNdDupClear

Table 1371: svcTlsProxyNdDupClear properties

Property name	Value
Application name	SVCMGR
Event ID	2349
Event name	svcTlsProxyNdDupClear
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.59
Default severity	minor
Message format string	A duplicate proxy ND entry *$svcTlsProxyNdIpAddr$* is cleared in service *$svcId$*
Cause	The svcTlsProxyNdDupDetect notification is generated when a duplicate ND entry is cleared.
Effect	The proxy ARP entry is deleted or is overwritten by static entry.
Recovery	None needed.

70.112 svcTlsProxyNdDupDetect

Table 1372: svcTlsProxyNdDupDetect properties

Property name	Value
Application name	SVCMGR
Event ID	2348
Event name	svcTlsProxyNdDupDetect
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.58

Property name	Value
Default severity	minor
Message format string	A duplicate proxy ND entry was detected with new MAC *$svcNotifTls ProxyMacAddr$* for entry IP *$svcTlsProxyArpIpAddr$* MAC *$svcTls ProxyArpMacAddr$* in service *$svcId$*
Cause	The svcTlsProxyNdDupDetect notification is generated when duplicate detection criteria is met when a new mac address overwrites the existing mac address for the proxy arp entry.
Effect	A traffic disruption may occur if both IP addresses are active.
Recovery	Identify the systems using the old MAC address and correct the configuration."

70.113 svcTlsProxyNdSvcHiUsgClr

Table 1373: svcTlsProxyNdSvcHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2365
Event name	svcTlsProxyNdSvcHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.75
Default severity	minor
Message format string	Service *$svcId$* has proxy ND entries below 90% of the per-service limit
Cause	The svcTlsProxyNdSvcHiUsgClr notification is generated when the number of proxy ND entries in a VPLS service drops below 90% of the per-service limit.
Effect	The VPLS service has reached 90% of the proxy ND entries limit.
Recovery	None needed.

70.114 svcTlsProxyNdSvcHiUsgSet

Table 1374: svcTlsProxyNdSvcHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2364
Event name	svcTlsProxyNdSvcHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.74
Default severity	minor
Message format string	Service *$svcId$* has proxy ND entries in excess of 95% of the per-service limit
Cause	The svcTlsProxyNdSvcHiUsgSet notification is generated when the number of proxy ND entries in a VPLS service exceeds 95% of the per-service limit.
Effect	The VPLS service has reached 95% of the proxy ND entries limit.
Recovery	None needed.

70.115 svcTlsProxyNdSysHiUsgClr

Table 1375: svcTlsProxyNdSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2363
Event name	svcTlsProxyNdSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.73
Default severity	minor
Message format string	The proxy ND entries is below 90% of the system limit
Cause	The svcTlsProxyNdSysHiUsgClr notification is generated when the number of proxy ND entries in the system drops below 90% of the system limit.
Effect	90% of the system proxy ND entries limit is reached.
Recovery	None needed.

70.116 svcTlsProxyNdSysHiUsgSet

Table 1376: svcTlsProxyNdSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2362
Event name	svcTlsProxyNdSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.72
Default severity	minor
Message format string	The proxy ND entries in the system exceeds 95% of the system limit
Cause	The svcTlsProxyNdSysHiUsgSet notification is generated when the number of proxy ND entries in the system exceeds 95% of the system limit.
Effect	95% of the system proxy ND entries limit is reached.
Recovery	None needed.

70.117 svcTlsSiteDesigFwdrChg

Table 1377: svcTlsSiteDesigFwdrChg properties

Property name	Value
Application name	SVCMGR
Event ID	2531
Event name	svcTlsSiteDesigFwdrChg
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.34
Default severity	warning
Message format string	Service-id *$svcId$* site *$svcTlsSiteIdName$* is *$svcTlsSite IdDesignatedFwdr$* the designated-forwarder
Cause	Designated-Forwarder status of the BGP multi-homing site associated with this service has changed.
Effect	N/A

Property name	Value
Recovery	N/A

70.118 svcTlsVTEPEgrVniSvcHiUsgAlarmClr

Table 1378: svcTlsVTEPEgrVniSvcHiUsgAlarmClr properties

Property name	Value
Application name	SVCMGR
Event ID	2340
Event name	svcTlsVTEPEgrVniSvcHiUsgAlarmClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.51
Default severity	minor
Message format string	Service *$svcId$* has VTEP-Egress VNIs below 90% of the per-service VTEP-Egress VNI multicast limit.
Cause	The svcTlsVTEPEgrVniSvcHiUsgAlarmClr notification is generated when the number of VTEP-Egress VNIs in a VPLS service drops below 90% of the per-service VTEP-Egress VNI multicast limit.
Effect	The VPLS service has reached 90% of the VTEP-Egress VNI multicast limit.
Recovery	None needed.

70.119 svcTlsVTEPEgrVniSvcHiUsgAlarmSet

Table 1379: svcTlsVTEPEgrVniSvcHiUsgAlarmSet properties

Property name	Value
Application name	SVCMGR
Event ID	2339
Event name	svcTlsVTEPEgrVniSvcHiUsgAlarmSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.50
Default severity	minor

Property name	Value
Message format string	Service *$svcId$* has VTEP-Egress VNIs in excess of 95% of the per-service VTEP-Egress VNI multicast limit.
Cause	The svcTlsVTEPEgrVniSvcHiUsgAlarmSet notification is generated when the number of VTEP-Egress VNIs in a VPLS service exceeds 95% of the per-service VTEP-Egress VNI multicast limit.
Effect	The VPLS service has reached 95% of the VTEP-Egress VNI multicast limit.
Recovery	None needed.

70.120 svcTlsVTEPEgrVniSysHiUsgAlarmClr

Table 1380: svcTlsVTEPEgrVniSysHiUsgAlarmClr properties

Property name	Value
Application name	SVCMGR
Event ID	2338
Event name	svcTlsVTEPEgrVniSysHiUsgAlarmClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.49
Default severity	minor
Message format string	The number of VTEP-Egress VNIs in the system is below 90% of the system VTEP-Egress VNI limit.
Cause	The svcTlsVTEPEgrVniSysHiUsgAlarmClr notification is generated when the number of VTEP-Egress VNIs in the system drops below 90% of the system VTEP-Egress VNI limit.
Effect	90% of the system VTEP-Egress VNI limit is reached.
Recovery	None needed.

70.121 svcTlsVTEPEgrVniSysHiUsgAlarmSet

Table 1381: svcTlsVTEPEgrVniSysHiUsgAlarmSet properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2337
Event name	svcTlsVTEPEgrVniSysHiUsgAlarmSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.48
Default severity	minor
Message format string	The number of VTEP-Egress VNIs in the system exceeds 95% of the system VTEP-Egress VNI limit.
Cause	The svcTlsVTEPEgrVniSysHiUsgAlarmSet notification is generated when the number of VTEP-Egress VNIs in the system exceeds 95% of the system VTEP-Egress VNI limit.
Effect	95% of the system VTEP-Egress VNI limit is reached.
Recovery	None needed.

70.122 svcTlsVTEPHiUsageAlarmCleared

Table 1382: svcTlsVTEPHiUsageAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2336
Event name	svcTlsVTEPHiUsageAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.47
Default severity	minor
Message format string	The number of VTEPs in the system is below 90% of the system VTEP limit.
Cause	The svcTlsVTEPHiUsageAlarmCleared notification is generated when the number of VTEPs in the system drops below 90% of system VTEP limit.
Effect	90% of the system VTEP limit is reached.
Recovery	None needed.

70.123 svcTlsVTEPHiUsageAlarmRaised

Table 1383: svcTlsVTEPHiUsageAlarmRaised properties

Property name	Value
Application name	SVCMGR
Event ID	2335
Event name	svcTlsVTEPHiUsageAlarmRaised
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.46
Default severity	minor
Message format string	The number of VTEPs in the system exceeds 95% of the system VTEP limit.
Cause	The svcTlsVTEPHiUsageAlarmRaised notification is generated when the number of VTEPs in the system exceeds 95% of the system VTEP limit.
Effect	95% of the system VTEP limit is reached.
Recovery	None needed.

70.124 svcTlsVxlanReplicatorChgd

Table 1384: svcTlsVxlanReplicatorChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2097
Event name	svcTlsVxlanReplicatorChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.84
Default severity	minor
Message format string	Assisted replicator in service *$svcId$* changed to VTEP *$svcTlsVTEPEgrVNIVTEPAddress$*, Egress VNI *$svc TlsVTEPEgrVNIEgrVNI$*.
Cause	The svcTlsVxlanReplicatorChgd notification is generated when there is a change in the replicator.
Effect	The replicator associated with a VPLS service is changed.

Property name	Value
Recovery	None needed.

70.125 svcVllSiteDesigFwdrChg

Table 1385: svcVllSiteDesigFwdrChg properties

Property name	Value
Application name	SVCMGR
Event ID	2545
Event name	svcVllSiteDesigFwdrChg
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.41
Default severity	warning
Message format string	Service-id *$svcId$* site *$svcVllSiteIdName$* is *$svcVllSiteIdDesignated Fwdr$* the designated-forwarder
Cause	Designated-Forwarder status of the BGP multi-homing site associated with this service has changed.
Effect	The new designated forwarder will be used to forward traffic.
Recovery	None needed.

70.126 tmnxEndPointTxActiveChanged

Table 1386: tmnxEndPointTxActiveChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2110
Event name	tmnxEndPointTxActiveChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.16
Default severity	warning
Message format string	The active object on endpoint " *$endPointName$*" in service *$endpoint SvcId$* changed to *$svcEndPointTxActiveString$*

Property name	Value
Cause	The transmit active object on an endpoint changed.
Effect	Traffic will now be forwarded on the new object unless the managed object svcEndPointTxActiveType is 'none'.
Recovery	N/A

70.127 tmnxIpTunnelOperRemIpChg

Table 1387: tmnxIpTunnelOperRemIpChg properties

Property name	Value
Application name	SVCMGR
Event ID	2547
Event name	tmnxIpTunnelOperRemIpChg
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.38
Default severity	minor
Message format string	Operational remote ipaddress for IP tunnel *$tmnxIpTunnelName$* has changed to *$tmnxIpTunnelOperRemIpAddr$*
Cause	The tmnxIpTunnelOperRemIpChg notification is generated when there is a change in operational remote address 'tmnxIpTunnelOperRem IpAddr' of the tunnel.
Effect	Operational state of the tunnel is not affected.
Recovery	Operator needs to look at the configuration of tmnxIpTunnelRemIpAddr and tmnxIpTunnelBackupRemIpAddr.

70.128 tmnxIpTunnelOperStateChange

Table 1388: tmnxIpTunnelOperStateChange properties

Property name	Value
Application name	SVCMGR
Event ID	2244
Event name	tmnxIpTunnelOperStateChange

Property name	Value
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.59
Default severity	minor
Message format string	Operational state change for IP Tunnel *$tmnxIpTunnelName$* on service *$svcId$* and SAP *$sapEncapValue$*, admin state: *$tmnxIpTunnelAdminState$*, oper state: *$tmnxIpTunnelOperState$*, oper flags: *$tmnxIpTunnelOperFlags$*
Cause	The tmnxIpTunnelOperStateChange notification is generated when there is a change in tmnxIpTunnelOperState for an IP tunnel.
Effect	When the tunnel is operationally down, traffic arriving at the tunnel endpoints will not be encapsulated and transported.
Recovery	N/A

70.129 tmnxSapStpExcepCondStateChng

Table 1389: tmnxSapStpExcepCondStateChng properties

Property name	Value
Application name	SVCMGR
Event ID	2044
Event name	tmnxSapStpExcepCondStateChng
SNMP notification prefix and OID	TIMETRA-SAP-MIB.tstpTraps.37
Default severity	minor
Message format string	TODO
Cause	The tmnxSapStpExcepCondStateChng notification is generated when the value of the object sapTlsStpException has changed, i.e. when the exception condition changes on the indicated SAP.
Effect	N/A
Recovery	N/A

70.130 tmnxStpRootGuardViolation

Table 1390: tmnxStpRootGuardViolation properties

Property name	Value
Application name	SVCMGR
Event ID	2043
Event name	tmnxStpRootGuardViolation
SNMP notification prefix and OID	TIMETRA-SAP-MIB.tstpTraps.35
Default severity	minor
Message format string	TODO
Cause	The tmnxStpRootGuardViolation notification is generated when a SAP which has root-guard configured is trying to become root (has a better STP priority vector). The SAP will become alternate and traffic will be blocked.
Effect	N/A
Recovery	N/A

70.131 tmnxSubAcctPlcyFailure

Table 1391: tmnxSubAcctPlcyFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2503
Event name	tmnxSubAcctPlcyFailure
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.4
Default severity	warning
Message format string	Radius accounting policy *$tmnxSubAcctPlcyName$* failure - *$tmnxSubAcctPlcyFailureReason$*.
Cause	A RADIUS accounting request was not sent out successfully to any of the RADIUS servers in the indicated accounting policy.
Effect	N/A
Recovery	N/A

70.132 tmnxSubAcctPlcyRadSerOperStatChg

Table 1392: tmnxSubAcctPlcyRadSerOperStatChg properties

Property name	Value
Application name	SVCMGR
Event ID	2506
Event name	tmnxSubAcctPlcyRadSerOperStatChg
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.7
Default severity	minor
Message format string	Subscriber Accounting RADIUS server *$tmnxSubAcctPlcyRadServ Addr$* operational status changed to *$tmnxSubAcctPlcyRadServOper State$*.
Cause	The operational status of a Radius server, configured for use with DHCP radius based subscriber accounting, has transitioned either from 'inService' to 'outOfService' or from 'outOfService' to 'inService'.
Effect	N/A
Recovery	No recovery is necessary.

70.133 tmnxSubAuthPlcyRadSerOperStatChg

Table 1393: tmnxSubAuthPlcyRadSerOperStatChg properties

Property name	Value
Application name	SVCMGR
Event ID	2505
Event name	tmnxSubAuthPlcyRadSerOperStatChg
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.6
Default severity	minor
Message format string	Subscriber Authentication RADIUS server *$tmnxSubAuthPlcyRadServ Address$* operational status changed to *$tmnxSubAuthPlcyRadServ OperState$*.

Property name	Value
Cause	The operational status of a Radius server, configured for use with DHCP radius authentication, has transitioned either from inService' to 'outOfService' or from 'outOfService' to 'inService'.
Effect	N/A
Recovery	No recovery is necessary.

70.134 tmnxSubBrgCreated

Table 1394: tmnxSubBrgCreated properties

Property name	Value
Application name	SVCMGR
Event ID	2564
Event name	tmnxSubBrgCreated
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.38
Default severity	warning
Message format string	The Bridged Residential Gateway with identifier *$tmnxSubBrgId$* has been created in the system.
Cause	The system issues the tmnxSubBrgCreated notification when it creates a conceptual row in the tmnxSubBrgTable.
Effect	The system is aware of a Bridged Residential Gateway and has context for it.
Recovery	Not required. This notification is informational.

70.135 tmnxSubBrgCvInitFailed

Table 1395: tmnxSubBrgCvInitFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2566
Event name	tmnxSubBrgCvInitFailed

Property name	Value
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.40
Default severity	warning
Message format string	Could not initiate connectivity verification of BRG *$tmnxSubBrgId$* using IP address *$tmnxSubNotifIpAddr$*
Cause	The system issues the tmnxSubBrgCvInitFailed notification when it does not have enough resources to start connectivity verification for a Bridged Residential Gateway (BRG) identified by tmnxSubBrgId, using the IP address tmnxSubNotifIpAddr in the virtual router instance with identifier vRtrID. Some hardware configurations may have insufficient resources to start and maintain connectivity verification for a huge number of Bridged Residential Gateways.
Effect	The system can only relay on the BRG host activity to determine if the BRG is connected.
Recovery	Not required.

70.136 tmnxSubBrgDeleted

Table 1396: tmnxSubBrgDeleted properties

Property name	Value
Application name	SVCMGR
Event ID	2565
Event name	tmnxSubBrgDeleted
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.39
Default severity	warning
Message format string	The Bridged Residential Gateway with identifier *$tmnxSubBrgId$* has been removed from the system.
Cause	The system issues the tmnxSubBrgDeleted notification when it destroys a conceptual row in the tmnxSubBrgTable. It may be the expected consequence of BRG inactivity, or may be caused by some kind of connectivity failure; this system cannot distinguish between these two causes.
Effect	The system has become unaware of a Bridged Residential Gateway.
Recovery	Recovery may or may not be required, depending of the cause.

70.137 tmnxSubBrgRadiusAuthError

Table 1397: tmnxSubBrgRadiusAuthError properties

Property name	Value
Application name	SVCMGR
Event ID	2569
Event name	tmnxSubBrgRadiusAuthError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.43
Default severity	warning
Message format string	Could not authenticate the Bridged Residential Gateway *$tmnxSubBrgId$ - $tmnxSubRadiusSubAuthReason$*
Cause	The tmnxSubBrgRadiusAuthError notification indicates that the system encountered a problem while trying to authenticate a Bridged Residential Gateway (BRG) with an Authentication, Authorization, and Accounting (AAA) management system using a protocol such as Radius or Diameter.
Effect	No hosts associated with the BRG are reachable via this system.
Recovery	Depends on the details of the failure.

70.138 tmnxSubBrgRadiusCoaError

Table 1398: tmnxSubBrgRadiusCoaError properties

Property name	Value
Application name	SVCMGR
Event ID	2568
Event name	tmnxSubBrgRadiusCoaError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.42
Default severity	warning
Message format string	Could not apply a Radius update for the Bridged Residential Gateway *$tmnxSubBrgId$ - $tmnxSubRadiusCoAReason$*

Property name	Value
Cause	The tmnxSubBrgRadiusCoaError notification indicates that the system was unable to process a Radius Change of Authorization (CoA) request for a Bridged Residential Gateway (BRG).
Effect	All hosts associated with the BRG use outdated parameters.
Recovery	Depends on the details of the failure.

70.139 tmnxSubBrgRadiusUpdateIpoeSeFail

Table 1399: tmnxSubBrgRadiusUpdateIpoeSeFail properties

Property name	Value
Application name	SVCMGR
Event ID	2567
Event name	tmnxSubBrgRadiusUpdateIpoeSeFail
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.41
Default severity	warning
Message format string	Could not apply a Radius update for the Bridged Residential Gateway *$tmnxSubBrgId$* to the IPoE session with MAC *$tmnxSubNotifMac Addr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSub AdditionalInfo$*
Cause	The system issues the tmnxSubBrgRadiusUpdateIpoeSeFail notification when it encounters a failure while processing a Radius update for a Bridged Residential Gateway (BRG), and a failure occors for one of the associated IPoE sessions. The BRG is identified by tmnx SubBrgId, the IPoE session by svcId, sapPortId, sapEncapValue and tmnxSubNotifMacAddr. More details about the failure are in tmnxSub AdditionalInfo.
Effect	A particular IPoE session has outdated parameters.
Recovery	Depends on the details of the failure.

70.140 tmnxSubBrgSessionLimitReached

Table 1400: tmnxSubBrgSessionLimitReached properties

Property name	Value
Application name	SVCMGR
Event ID	2570
Event name	tmnxSubBrgSessionLimitReached
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.44
Default severity	warning
Message format string	Bridged Residential Gateway *$tmnxSubBrgId$* exceeded its limit of 128 IPoE sessions
Cause	The system issues the tmnxSubBrgSessionLimitReached notification when this system fails to create an IPoE session associated with the Bridged Residential Gateway identified by tmnxSubBrgId because its IPoE session limit is exceeded. The IPoE session limit is 128 sessions per BRG.
Effect	The system can not set up the IPoE session.
Recovery	Not required. This notification is informational.

70.141 tmnxSubHostInconsistentAtmTdOvr

Table 1401: tmnxSubHostInconsistentAtmTdOvr properties

Property name	Value
Application name	SVCMGR
Event ID	2536
Event name	tmnxSubHostInconsistentAtmTdOvr
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.20
Default severity	warning
Message format string	Inconsistent ATM traffic descriptor given by AAA server for a host of subscriber *$tmnxSubHostInfoV2SubIdent$ - $tmnxSubAdditionalInfo$*
Cause	"The AAA server specifies different ATM profile descriptors for subscriber hosts on the same ATM Virtual Circuit."

Property name	Value
Effect	"The ATM traffic descriptor of the first host on the ATM Virtual Circuit is used for all subsequent hosts."
Recovery	"The AAA server configuration should be made consistent."

70.142 tmnxSubHostInfoConflict

Table 1402: tmnxSubHostInfoConflict properties

Property name	Value
Application name	SVCMGR
Event ID	2562
Event name	tmnxSubHostInfoConflict
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.36
Default severity	warning
Message format string	There was a conflict in the parameter set of host MAC *$tmnxSubNotif MacAddr$* of subscriber *$tmnxSubIdent$* - *$tmnxSubAdditionalInfo$*
Cause	The system may issue the tmnxSubHostInfoConflict notification when it detects a conflict while processing the parameters to be applied to a new subscriber host.
Effect	The host is set up, but with unexpected values for some parameters.
Recovery	None.

70.143 tmnxSubHostLcktLimitReached

Table 1403: tmnxSubHostLcktLimitReached properties

Property name	Value
Application name	SVCMGR
Event ID	2548
Event name	tmnxSubHostLcktLimitReached
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.22
Default severity	minor

Property name	Value
Message format string	Maximum number of *$tmnxSubAdditionalInfo$* locked out hosts is reached on this system.
Cause	"The tmnxSubHostLcktLimitReached notification indicates that the system wide maximum number of lockout hosts is reached."
Effect	"Todo."
Recovery	"Todo."

70.144 tmnxSubHostLcktSapLimitReached

Table 1404: tmnxSubHostLcktSapLimitReached properties

Property name	Value
Application name	SVCMGR
Event ID	2549
Event name	tmnxSubHostLcktSapLimitReached
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.23
Default severity	minor
Message format string	Maximum number of *$tmnxSubLcktPlcyMaxLcktHosts$* locked out hosts is reached on host *$tmnxSubNotifMacAddr$*.
Cause	"The tmnxSubHostLcktSapLimitReached notification indicates that the maximum number of lockout hosts on a given SAP is reached."
Effect	"Todo."
Recovery	N/A

70.145 tmnxSubIpoeInvalidCidRidChange

Table 1405: tmnxSubIpoeInvalidCidRidChange properties

Property name	Value
Application name	SVCMGR
Event ID	2555
Event name	tmnxSubIpoeInvalidCidRidChange

Property name	Value
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.29
Default severity	warning
Message format string	IPoE session CID/RID change failure for host with MAC address *$tmnxSubNotifMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	The IPoE session CID or RID change is invalid.
Effect	The system can not setup the IPoE session.
Recovery	No recovery is required on this system.

70.146 tmnxSubIpoeInvalidSessionKey

Table 1406: tmnxSubIpoeInvalidSessionKey properties

Property name	Value
Application name	SVCMGR
Event ID	2554
Event name	tmnxSubIpoeInvalidSessionKey
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.28
Default severity	warning
Message format string	IPoE session key failure for host with MAC address *$tmnxSubNotifMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	The IPoE session key is invalid.
Effect	The system can not setup the IPoE session.
Recovery	No recovery is required on this system.

70.147 tmnxSubIpoeMigrHostDeleted

Table 1407: tmnxSubIpoeMigrHostDeleted properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2559
Event name	tmnxSubIpoeMigrHostDeleted
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.33
Default severity	warning
Message format string	IPoE session migration deleted host *$tmnxSubNotifIpAddr$*/*$tmnxSubNotifPrefixLength$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	The system is performing an IPoE session migration.
Effect	The host will be migrated.
Recovery	No recovery is required on this system.

70.148 tmnxSubIpoePersistenceRecovery

Table 1408: tmnxSubIpoePersistenceRecovery properties

Property name	Value
Application name	SVCMGR
Event ID	2557
Event name	tmnxSubIpoePersistenceRecovery
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.32
Default severity	warning
Message format string	IPoE session persistence recovery failure for host with MAC address *$tmnxSubNotifMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	The system is still recovering from persistence.
Effect	The system can not setup the IPoE session.
Recovery	No recovery is required on this system.

70.149 tmnxSubIpoeSessionLimitReached

Table 1409: tmnxSubIpoeSessionLimitReached properties

Property name	Value
Application name	SVCMGR
Event ID	2556
Event name	tmnxSubIpoeSessionLimitReached
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.31
Default severity	warning
Message format string	IPoE session limit failure for host with MAC address *$tmnxSubNotif MacAddr$* on SAP *$sapEncapValue$* in service *$svcId$ - $tmnxSub AdditionalInfo$*
Cause	The IPoE session limit is reached.
Effect	The system can not setup the IPoE session.
Recovery	No recovery is required on this system.

70.150 tmnxSubMcsRelatedProblem

Table 1410: tmnxSubMcsRelatedProblem properties

Property name	Value
Application name	SVCMGR
Event ID	2504
Event name	tmnxSubMcsRelatedProblem
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.5
Default severity	warning
Message format string	Problem encountered in Subscriber Management, while performing Multi Chassis Syncing: *$tmnxSubMcsRelatedProblemDescr$*
Cause	A subscriber management specific problem occured during Multi Chassis Syncing, e.g. of DHCP lease states. The problem is described in the object tmnxSubMcsRelatedProblemDescr.
Effect	N/A
Recovery	N/A

70.151 tmnxSubMngdHostCreationFail

Table 1411: tmnxSubMngdHostCreationFail properties

Property name	Value
Application name	SVCMGR
Event ID	2560
Event name	tmnxSubMngdHostCreationFail
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.34
Default severity	warning
Message format string	Could not create host IP *$tmnxSubNotifIpAddr$* MAC *$tmnxSubNotifMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	A failure occurs while trying to create a managed host. The object tmnxSubAdditionalInfo provides more information about the failure.
Effect	The context for the managed host is not created. The system cannot provide network connectivity to the host.
Recovery	The recovery action depends on the root cause of the failure. The root cause may be a misconfiguration in the client device, the access network, in this system, or in the AAA server configuration.

70.152 tmnxSubMngdHostOverride

Table 1412: tmnxSubMngdHostOverride properties

Property name	Value
Application name	SVCMGR
Event ID	2561
Event name	tmnxSubMngdHostOverride
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.35
Default severity	warning
Message format string	Existing managed host IP *$tmnxSubMngdHostIpAddr$* MAC *$tmnxSubMngdHostMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* overridden - *$tmnxSubAdditionalInfo$*

Property name	Value
Cause	The tmnxSubMngdHostOverride notification is sent when a new managed host replaces an existing host with the same IP address.
Effect	The existing host is removed from the system.
Recovery	None.

70.153 tmnxSubPlBndFailed

Table 1413: tmnxSubPlBndFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2563
Event name	tmnxSubPlBndFailed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.37
Default severity	warning
Message format string	Could not create an IP address binding in home-aware pool *$tmnxSubNotifName$* for the host with MAC *$tmnxSubNotifMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	The system issues the tmnxSubPlBndFailed notification upon a failed attempt to create a subscriber home-aware pool MAC / IP address binding.
Effect	The host with the MAC address indicated by tmnxSubNotifMacAddr could not get an IP address from the home-aware pool indicated by tmnxSubNotifName, and cannot get IP connectivity through this system.
Recovery	The content of tmnxSubAdditionalInfo may contain more details about the failure reason and hence suggest a possible recovery action.

70.154 tmnxSubRadSapCoAError

Table 1414: tmnxSubRadSapCoAError properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2511
Event name	tmnxSubRadSapCoAError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.10
Default severity	warning
Message format string	Problem encountered in Subscriber Management, while processing a CoA request on SAP *$sapEncapValue$* in service *$svcId$* from a Radius server: *$tmnxSubRadiusCoAReason$*
Cause	The system was unable to process a Change of Authorization (CoA) equest from a Radius server.
Effect	N/A
Recovery	N/A

70.155 tmnxSubRadSapDisconnectError

Table 1415: tmnxSubRadSapDisconnectError properties

Property name	Value
Application name	SVCMGR
Event ID	2509
Event name	tmnxSubRadSapDisconnectError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.8
Default severity	warning
Message format string	Problem encountered in Subscriber Management, while processing a Disconnect request on SAP *$sapEncapValue$* in service *$svcId$* from a Radius server: *$tmnxSubRadiusDisconnectReason$*
Cause	The system was unable to process a Disconnect request from a Radius server.
Effect	N/A
Recovery	N/A

70.156 tmnxSubRadSapSubAuthError

Table 1416: tmnxSubRadSapSubAuthError properties

Property name	Value
Application name	SVCMGR
Event ID	2513
Event name	tmnxSubRadSapSubAuthError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.12
Default severity	warning
Message format string	Problem encountered in Subscriber Management, subscriber authentication error on SAP *$sapEncapValue$* in service *$svcId$*: *$tmnxSubRadiusSubAuthReason$*
Cause	The system encountered a problem while trying to authenticate a subscriber.
Effect	N/A
Recovery	N/A

70.157 tmnxSubRadSdpBndCoAError

Table 1417: tmnxSubRadSdpBndCoAError properties

Property name	Value
Application name	SVCMGR
Event ID	2512
Event name	tmnxSubRadSdpBndCoAError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.11
Default severity	warning
Message format string	Problem encountered in Subscriber Management, while processing a CoA request on SDP Bind *$sdpBindId$* in service *$svcId$* from a Radius server: *$tmnxSubRadiusCoAReason$*
Cause	The system was unable to process a Change of Authorization (CoA) request from a Radius server on a SDP Binding.
Effect	N/A

Property name	Value
Recovery	No recovery is necessary.

70.158 tmnxSubRadSdpBndDisconnectError

Table 1418: tmnxSubRadSdpBndDisconnectError properties

Property name	Value
Application name	SVCMGR
Event ID	2510
Event name	tmnxSubRadSdpBndDisconnectError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.9
Default severity	warning
Message format string	Problem encountered in Subscriber Management, while processing a Disconnect request on SDP Bind *$sdpBindId$* in service *$svcId$* from a Radius server: *$tmnxSubRadiusDisconnectReason$*
Cause	The system was unable to process a Disconnect request from a Radius server.
Effect	N/A
Recovery	N/A

70.159 tmnxSubRadSdpBndSubAuthError

Table 1419: tmnxSubRadSdpBndSubAuthError properties

Property name	Value
Application name	SVCMGR
Event ID	2514
Event name	tmnxSubRadSdpBndSubAuthError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.13
Default severity	warning

Property name	Value
Message format string	Problem encountered in Subscriber Management, subscriber authentication error on SDP Bind *$sdpBindId$* in service *$svcId$*: *$tmnxSubRadiusSubAuthReason$*
Cause	The system encountered a problem while trying to authenticate a subscriber on an SDP Binding.
Effect	N/A
Recovery	No recovery is necessary.

70.160 tmnxSubscriberCreated

Table 1420: tmnxSubscriberCreated properties

Property name	Value
Application name	SVCMGR
Event ID	2500
Event name	tmnxSubscriberCreated
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.1
Default severity	warning
Message format string	Subscriber *$tmnxSubIdent$* has been created in the system
Cause	A new subscriber was added to the tmnxSubscriberInfoTable.
Effect	The subscriber is henceforward known in the system.
Recovery	No recovery is necessary.

70.161 tmnxSubscriberDeleted

Table 1421: tmnxSubscriberDeleted properties

Property name	Value
Application name	SVCMGR
Event ID	2501
Event name	tmnxSubscriberDeleted

Property name	Value
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.2
Default severity	warning
Message format string	Subscriber *$tmnxSubIdent$* has been removed from the system
Cause	A subscriber was removed from the tmnxSubscriberInfoTable
Effect	The subscriber is henceforward no longer known in the system.
Recovery	No recovery is necessary.

70.162 tmnxSubscriberRenamed

Table 1422: tmnxSubscriberRenamed properties

Property name	Value
Application name	SVCMGR
Event ID	2502
Event name	tmnxSubscriberRenamed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.3
Default severity	warning
Message format string	Subscriber *$tmnxOldSubIdent$* has been renamed to *$tmnxNewSubIdent$*.
Cause	An existing subscriber was renamed.
Effect	The subscriber is henceforward known under a different name.
Recovery	No recovery is necessary.

70.163 tmnxSubSlaacOverride

Table 1423: tmnxSubSlaacOverride properties

Property name	Value
Application name	SVCMGR
Event ID	2022

Property name	Value
Event name	tmnxSubSlaacOverride
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.25
Default severity	warning
Message format string	TODO
Cause	The tmnxSubSlaacOverride notification is sent when an IPv6 client requests a DHCPv6 non-temporary address (IA_NA) which overrides an existing SLAAC prefix for this client.
Effect	The SLAAC host is removed from the system.
Recovery	None

70.164 tmnxSubSlaacSetupFailure

Table 1424: tmnxSubSlaacSetupFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2546
Event name	tmnxSubSlaacSetupFailure
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.21
Default severity	warning
Message format string	Failed to update SLAAC host on *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	"Failed to update or create a SLAAC host in tmnxSubSlaacTable."
Effect	"Entries in tmnxSubSlaacTable are not updated."
Recovery	"Subscriber Management Configuration should be changed to recover from the failure described in tmnxSubAdditionalInfo."

70.165 tmnxSubSysChassMemoryUsageHi

Table 1425: tmnxSubSysChassMemoryUsageHi properties

Property name	Value
Application name	SVCMGR
Event ID	2551
Event name	tmnxSubSysChassMemoryUsageHi
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.26
Default severity	minor
Message format string	The subscriber management's memory usage high status in chassis *$tmnxChassisIndex$* changed to *$tmnxSubSysChassMemoryUsage High$*.
Cause	The tmnxSubSysChassMemoryUsageHi notification is sent when the memory usage by subscriber management on this system reaches its high watermark ('true') or a chassis or when it reaches its low watermark again ('false').
Effect	There is no immediate effect, but when the usage actually hits the limit, new hosts will not be created.
Recovery	Either change the network configuration to offload subscribers to other systems, or upgrade to a set of newer CPM (system management processor) with more memory.

70.166 tmnxSubUserCategoryError

Table 1426: tmnxSubUserCategoryError properties

Property name	Value
Application name	SVCMGR
Event ID	2530
Event name	tmnxSubUserCategoryError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.16
Default severity	minor
Message format string	An error was encountered in credit control for host *$tmnxSubNotif IpAddr$* with MAC address *$tmnxSubNotifMacAddr$* on SAP: *$sap EncapValue$*, service:*$svcId$*. Subscriber: *$tmnxSubIdent$*. SLA Profile: *$tmnxSubNotifSLAProfName$*. Category Map name: *$tmnxSub*

Property name	Value
	NotifApCMapName$*. Category name: *$tmnxSubNotifApCategoryName$*. More info: *$tmnxSubAdditionalInfo$
Cause	N/A
Effect	N/A
Recovery	N/A

70.167 tmnxSubUserCategoryOutOfCredit

Table 1427: tmnxSubUserCategoryOutOfCredit properties

Property name	Value
Application name	SVCMGR
Event ID	2527
Event name	tmnxSubUserCategoryOutOfCredit
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.14
Default severity	minor
Message format string	The credit has expired for host *$tmnxSubNotifIpAddr$* with MAC address *$tmnxSubNotifMacAddr$* on SAP: *$sapEncapValue$*, service:*$svcId$*. Subscriber: *$tmnxSubIdent$*. SLA Profile: *$tmnxSubNotifSLAProfName$*. Category Map name: *$tmnxSubNotifApCMapName$*. Category name: *$tmnxSubNotifApCategoryName$*.
Cause	N/A
Effect	N/A
Recovery	N/A

70.168 tmnxSubUserCategoryRefreshCredit

Table 1428: tmnxSubUserCategoryRefreshCredit properties

Property name	Value
Application name	SVCMGR
Event ID	2529

Property name	Value
Event name	tmnxSubUserCategoryRefreshCredit
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.15
Default severity	minor
Message format string	The credit refresh has been initiated for host *$tmnxSubNotifIpAddr$* with MAC address *$tmnxSubNotifMacAddr$* on SAP: *$sapEncapValue $*, service:*$svcId$*. Subscriber: *$tmnxSubIdent$*. SLA Profile: *$tmnx SubNotifSLAProfName$*. Category Map name: *$tmnxSubNotifApCMap Name$*. Category name: *$tmnxSubNotifApCategoryName$*.
Cause	N/A
Effect	N/A
Recovery	N/A

70.169 tmnxSubVSubnetHostsDeleted

Table 1429: tmnxSubVSubnetHostsDeleted properties

Property name	Value
Application name	SVCMGR
Event ID	2552
Event name	tmnxSubVSubnetHostsDeleted
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.27
Default severity	warning
Message format string	All hosts deleted of subscriber *$tmnxSubInfoSubIdent$* in service *$svcId$* because of a new gateway IP/subnet assignment *$tmnx SubVSubnetDefRtrAddr$*/*$tmnxSubVSubnetPrefixLength$*
Cause	The tmnxSubVSubnetHostsDeleted notification is sent when this system deletes all host contexts of a subscriber associated with a virtual subnet because a new default router and/or subnet were assigned. This is the consequence of a change in the configuration in the server that assigns the subnets.
Effect	The hosts have to transmit DHCP requests if they need a connection.
Recovery	None.

71 SYSTEM

71.1 persistenceRestoreProblem

Table 1430: persistenceRestoreProblem properties

Property name	Value
Application name	SYSTEM
Event ID	2041
Event name	persistenceRestoreProblem
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.41
Default severity	minor
Message format string	Problem occured while processing persistence record for *$tmnx PersistencyClient$ - $tmnxPersistencyNotifyMsg$*
Cause	The persistenceRestoreProblem notification is generated when an an error is detected while processing a persistence record.
Effect	N/A
Recovery	N/A

71.2 persistencyClosedAlarmCleared

Table 1431: persistencyClosedAlarmCleared properties

Property name	Value
Application name	SYSTEM
Event ID	2031
Event name	persistencyClosedAlarmCleared
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.31
Default severity	major

Property name	Value
Message format string	Persistency-file on Card *$tmnxPersistenceAffectedCpm$* for *$tmnx PersistencyClient$* on device *$tmnxPersistencyFileLocator$* is re-opened.*$tmnxPersistencyNotifyMsg$*
Cause	The output device used to store the persistence data is available for use again.
Effect	N/A
Recovery	N/A

71.3 persistencyClosedAlarmRaised

Table 1432: persistencyClosedAlarmRaised properties

Property name	Value
Application name	SYSTEM
Event ID	2030
Event name	persistencyClosedAlarmRaised
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.30
Default severity	major
Message format string	Persistency-file on Card *$tmnxPersistenceAffectedCpm$* for *$tmnx PersistencyClient$* on device *$tmnxPersistencyFileLocator$* is closed. Persistency across system reboot is no longer guaranteed. *$tmnx PersistencyNotifyMsg$*
Cause	The system was unable to store persistency data (e.g. because the storage device is inaccessible, or full)."
Effect	N/A
Recovery	N/A

71.4 persistencyEventReport

Table 1433: persistencyEventReport properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2037
Event name	persistencyEventReport
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.37
Default severity	warning
Message format string	persistency event: *$tmnxPersistencyNotifyMsg$*
Cause	The system reported a subscriber management persistence event (e.g. the start and completion of a recovery action after system startup).
Effect	N/A
Recovery	N/A

71.5 persistencyFileSysThresCleared

Table 1434: persistencyFileSysThresCleared properties

Property name	Value
Application name	SYSTEM
Event ID	2051
Event name	persistencyFileSysThresCleared
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.51
Default severity	major
Message format string	Filesystem on Card *$tmnxPersistenceAffectedCpm$* for *$tmnx PersistencyClient$* on device *$tmnxPersistencyFileLocator$* has dropped below threshold level of 90 percent. *$tmnxPersistencyNotify Msg$*
Cause	The persistencyFileSysThresCleared notification is generated when the filesystem drops below 90 percent occupation.
Effect	N/A
Recovery	N/A

71.6 persistencyFileSysThresRaised

Table 1435: persistencyFileSysThresRaised properties

Property name	Value
Application name	SYSTEM
Event ID	2050
Event name	persistencyFileSysThresRaised
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.50
Default severity	major
Message format string	Filesystem on Card *$tmnxPersistenceAffectedCpm$* for *$tmnx PersistencyClient$* on device *$tmnxPersistencyFileLocator$* has reached threshold level of 90 percent. *$tmnxPersistencyNotifyMsg$*
Cause	The persistencyFileSysThresRaised notification is generated when the filesystem reaches 90 percent occupation.
Effect	N/A
Recovery	N/A

71.7 sbiBootConfig

Table 1436: sbiBootConfig properties

Property name	Value
Application name	SYSTEM
Event ID	2004
Event name	sbiBootConfig
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.4
Default severity	major
Message format string	Bootup configuration complete. Configuration status: *$sbiConfigStatus $*. SNMP Persistent Indexes status: *$sbiPersistStatus$*. System configured with persistent indexes: *$sbiPersistIndex$*.
Cause	The configuration phase following a system reboot has completed.
Effect	N/A

Property name	Value
Recovery	No recovery is necessary.

71.8 sbiBootConfigFailFileError

Table 1437: sbiBootConfigFailFileError properties

Property name	Value
Application name	SYSTEM
Event ID	2038
Event name	sbiBootConfigFailFileError
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.38
Default severity	major
Message format string	Unable to access the boot-bad-exec file *$sbiBootConfigFailScript$*
Cause	The bootup failed script file is not accessible.
Effect	N/A
Recovery	No recovery is necessary.

71.9 sbiBootConfigOKFileError

Table 1438: sbiBootConfigOKFileError properties

Property name	Value
Application name	SYSTEM
Event ID	2039
Event name	sbiBootConfigOKFileError
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.39
Default severity	major
Message format string	Unable to access the boot-good-exec file *$sbiBootConfigOKScript$*
Cause	The bootup configuration OK script file was not accessible.
Effect	N/A

Property name	Value
Recovery	No recovery is necessary.

71.10 sbiBootSnmpd

Table 1439: sbiBootSnmpd properties

Property name	Value
Application name	SYSTEM
Event ID	2005
Event name	sbiBootSnmpd
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.5
Default severity	major
Message format string	SNMP daemon initialization complete. System configured with persistent SNMP indexes: *$sbiPersistIndex$*. SNMP daemon admimistrative status: *$sbiSnmpdAdminStatus$*. SNMP daemon operational status: *$sbiSnmpdOperStatus$*.
Cause	The SNMP daemon initialization completed following a system reboot. Some system configuration and initialization errors might have resulted in the SNMP daemon being suspended.
Effect	N/A
Recovery	No recovery is necessary.

71.11 schedActionFailure

Table 1440: schedActionFailure properties

Property name	Value
Application name	SYSTEM
Event ID	2101
Event name	schedActionFailure
SNMP notification prefix and OID	DISMAN-SCHEDULE-MIB.schedTraps.1
Default severity	major

Property name	Value
Message format string	Schedule "*$schedName$*" created by " *$schedOwner$*" failed with error: *$schedFailureText$*
Cause	The invocation of a scheduled script-policy failed.
Effect	N/A
Recovery	N/A

71.12 smScriptAbort

Table 1441: smScriptAbort properties

Property name	Value
Application name	SYSTEM
Event ID	2102
Event name	smScriptAbort
SNMP notification prefix and OID	DISMAN-SCRIPT-MIB.smTraps.1
Default severity	major
Message format string	The *$tmnxSmRunExtAuthType$* operation failed or was aborted with error: *$smRunError$*. Run #*$smRunIndex$* of script-policy "*$smLaunchName$*" created by owner " *$smLaunchOwner$*" was executed with the user account "*$tmnxSmRunExtUserName$*".
Cause	A running script terminated with an smRunExitCode not equal to `no Error'.
Effect	N/A
Recovery	N/A

71.13 smScriptException

Table 1442: smScriptException properties

Property name	Value
Application name	SYSTEM
Event ID	2104

Property name	Value
Event name	smScriptException
SNMP notification prefix and OID	DISMAN-SCRIPT-MIB.smTraps.3
Default severity	minor
Message format string	The *$tmnxSmRunExtAuthType$* operation completed with an exception: *$smRunError$*. Run *#$smRunIndex$* of script-policy "*$sm LaunchName$*" created by owner " *$smLaunchOwner$*" was executed with the user account "*$tmnxSmRunExtUserName$*"
Cause	A script run completed with an error. This event can be used by scripts to notify other management applications about script errors. This event is not automatically generated by the Script MIB implementation. It is the responsibility of the executing script or the runtime system to emit this notification where it is appropriate to do so.
Effect	N/A
Recovery	N/A

71.14 smScriptResult

Table 1443: smScriptResult properties

Property name	Value
Application name	SYSTEM
Event ID	2103
Event name	smScriptResult
SNMP notification prefix and OID	DISMAN-SCRIPT-MIB.smTraps.2
Default severity	minor
Message format string	The *$tmnxSmRunExtAuthType$* operation completed with the result: *$smRunResult$*. Run *#$smRunIndex$* of script-policy "*$smLaunch Name$*" created by owner " *$smLaunchOwner$*" was executed with the user account "*$tmnxSmRunExtUserName$*".
Cause	A script run completed. This event can be used by scripts to notify other management applications about results \ produced by the script. This event is not automatically generated by the Script MIB implementation. It is the responsibility of the executing script to emit this notification where it is appropriate to do so.
Effect	N/A

Property name	Value
Recovery	N/A

71.15 sntpTimeDiffExceedsThreshold

Table 1444: sntpTimeDiffExceedsThreshold properties

Property name	Value
Application name	SYSTEM
Event ID	2018
Event name	sntpTimeDiffExceedsThreshold
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.18
Default severity	major
Message format string	Time differential between the SNTP server *$sntp_ip_address$* and the system exceeds 10 seconds
Cause	The time differential between the system and the SNTP server was more than 10 seconds. In this case the system clock was not automatically adjusted.
Effect	N/A
Recovery	N/A

71.16 socket_bind_failed

Table 1445: socket_bind_failed properties

Property name	Value
Application name	SYSTEM
Event ID	2016
Event name	socket_bind_failed
SNMP notification prefix and OID	N/A
Default severity	critical
Message format string	Could not bind to a socket

Property name	Value
Cause	A socket bind failed. There may be no sockets left in the system.
Effect	Cannot start new telnet/ftp sessions.
Recovery	Shutdown tasks that are consuming sockets.

71.17 socket_conn_accept_failed

Table 1446: socket_conn_accept_failed properties

Property name	Value
Application name	SYSTEM
Event ID	2017
Event name	socket_conn_accept_failed
SNMP notification prefix and OID	N/A
Default severity	critical
Message format string	Could not accept a new connection
Cause	A socket connection attempt failed. There may be no sockets left in the system.
Effect	Cannot start new telnet/ftp sessions.
Recovery	Shutdown tasks that are consuming sockets.

71.18 ssiSaveConfigFailed

Table 1447: ssiSaveConfigFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2003
Event name	ssiSaveConfigFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.3
Default severity	critical

Property name	Value
Message format string	Configuration file write failed: *$fileName$ $reason$*
Cause	The saving of configuration was stopped due to errors.
Effect	The configuration file could not be saved.
Recovery	No recovery is necessary.

71.19 ssiSaveConfigSucceeded

Table 1448: ssiSaveConfigSucceeded properties

Property name	Value
Application name	SYSTEM
Event ID	2002
Event name	ssiSaveConfigSucceeded
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.2
Default severity	major
Message format string	Configuration file saved to: *$fileName$*
Cause	The saving of configuration finished without errors.
Effect	Configuration file was saved.
Recovery	No recovery is necessary.

71.20 ssiSyncBootEnvFailed

Table 1449: ssiSyncBootEnvFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2015
Event name	ssiSyncBootEnvFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.17
Default severity	critical

Property name	Value
Message format string	Synchronization of boot environment files failed - *$tmnxSyncFailure Reason$*
Cause	The synchronization of boot environment files was stopped due to errors.
Effect	Boot environment files were not synchronized.
Recovery	No recovery is necessary.

71.21 ssiSyncBootEnvOK

Table 1450: ssiSyncBootEnvOK properties

Property name	Value
Application name	SYSTEM
Event ID	2014
Event name	ssiSyncBootEnvOK
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.16
Default severity	warning
Message format string	Boot environment files have been successfully synchronized
Cause	The synchronization of boot environment files finished without errors.
Effect	Boot environment files were synchronized.
Recovery	No recovery is necessary.

71.22 ssiSyncCertFailed

Table 1451: ssiSyncCertFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2049
Event name	ssiSyncCertFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.49

Property name	Value
Default severity	major
Message format string	Synchronization of certificate file(s) failed - *$tmnxSyncFailureReason$*
Cause	The ssiSyncCertFailed event is generated when the synchronization of certificate files between the primary and secondary CPMs is stopped due to errors. The tmnxSyncFailureReason will state the reason for the failure.
Effect	Cert files are not synchronized.
Recovery	The user should try to determine the cause of the failure and can attempt synchronizing the files again.

71.23 ssiSyncCertOK

Table 1452: ssiSyncCertOK properties

Property name	Value
Application name	SYSTEM
Event ID	2048
Event name	ssiSyncCertOK
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.48
Default severity	warning
Message format string	Cert file(s) have been successfully synchronized
Cause	The ssiSyncCertOK event is generated when the synchronization of certificate files between the primary and secondary CPMs finishes without errors.
Effect	Cert files are synchronized.
Recovery	No recovery is necessary.

71.24 ssiSyncConfigFailed

Table 1453: ssiSyncConfigFailed properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2013
Event name	ssiSyncConfigFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.15
Default severity	critical
Message format string	Synchronization of configuration files failed - *$tmnxSyncFailureReason $*
Cause	The synchronization of configuration files was stopped due to errors.
Effect	Configuration files were not synchronized.
Recovery	No recovery is necessary.

71.25 ssiSyncConfigOK

Table 1454: ssiSyncConfigOK properties

Property name	Value
Application name	SYSTEM
Event ID	2012
Event name	ssiSyncConfigOK
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.14
Default severity	warning
Message format string	Configuration files have been successfully synchronized
Cause	The synchronization of configuration files finished without errors.
Effect	Configuration files are synchronized.
Recovery	No recovery is necessary.

71.26 ssiSyncRollbackFailed

Table 1455: ssiSyncRollbackFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2047
Event name	ssiSyncRollbackFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.47
Default severity	critical
Message format string	Synchronization of rollback file(s) failed - *$tmnxSyncFailureReason$*
Cause	The ssiSyncRollbackFailed event is generated when the synchronization of rollback files between the primary and secondary CPMs is stopped due to errors. The tmnxSyncFailureReason will state the reason for the failure.
Effect	Rollback files are not synchronized.
Recovery	The user should try to determine the cause of the failure and can attempt synchronizing the files again.

71.27 ssiSyncRollbackOK

Table 1456: ssiSyncRollbackOK properties

Property name	Value
Application name	SYSTEM
Event ID	2046
Event name	ssiSyncRollbackOK
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.46
Default severity	warning
Message format string	Rollback file(s) have been successfully synchronized
Cause	The ssiSyncRollbackOK event is generated when the synchronization of rollback files between the primary and secondary CPMs finishes without errors.
Effect	Rollback files are synchronized.

Property name	Value
Recovery	No recovery is necessary.

71.28 stiDateAndTimeChanged

Table 1457: stiDateAndTimeChanged properties

Property name	Value
Application name	SYSTEM
Event ID	2001
Event name	stiDateAndTimeChanged
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.1
Default severity	warning
Message format string	Date and time on the system is *$stiDateAndTime$*
Cause	The stiDateAndTimeChanged notification is generated when the time on the system is explicity set.
Effect	The time on the system has been modified.
Recovery	No recovery is necessary.

71.29 stiDateAndTimeChanging

Table 1458: stiDateAndTimeChanging properties

Property name	Value
Application name	SYSTEM
Event ID	2081
Event name	stiDateAndTimeChanging
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.86
Default severity	warning
Message format string	Date and time on the system is changing from *$stiDateAndTime$*
Cause	The stiDateAndTimeChanging notification is generated when the time on the node is explicitly set. It is raised before the time is changed so

Property name	Value
	that the time of the change can be related to the original timescale. It shall be followed by the stiDateAndTimeChanged notification.
Effect	The time on the system is being changed.
Recovery	No recovery is necessary.

71.30 tmnxConfigConflict

Table 1459: tmnxConfigConflict properties

Property name	Value
Application name	SYSTEM
Event ID	2058
Event name	tmnxConfigConflict
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.58
Default severity	minor
Message format string	*$tmnxNotifyObjectName$* configuration conflict
Cause	A configuration attribute associated with a row entry in a MIB table is in conflict with another attribute. This event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

71.31 tmnxConfigCreate

Table 1460: tmnxConfigCreate properties

Property name	Value
Application name	SYSTEM
Event ID	2007
Event name	tmnxConfigCreate
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9

Property name	Value
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* managed object created
Cause	A new row entry was created in one of the MIB tables. This event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

71.32 tmnxConfigDelete

Table 1461: tmnxConfigDelete properties

Property name	Value
Application name	SYSTEM
Event ID	2008
Event name	tmnxConfigDelete
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.10
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* managed object deleted
Cause	A existing row entry in one of the MIB tables was deleted. This event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

71.33 tmnxConfigModify

Table 1462: tmnxConfigModify properties

Property name	Value
Application name	SYSTEM
Event ID	2006

Property name	Value
Event name	tmnxConfigModify
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.8
Default severity	warning
Message format string	*$tmnxNotifyObjectName$* configuration modified
Cause	A configuration attribute associated with a row entry in a MIB table was modified. This event can be used by the NMS to trigger maintenance polls of the configuration information.
Effect	N/A
Recovery	No recovery is necessary.

71.34 tmnxEhsDroppedByMinDelay

Table 1463: tmnxEhsDroppedByMinDelay properties

Property name	Value
Application name	SYSTEM
Event ID	2070
Event name	tmnxEhsDroppedByMinDelay
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.71
Default severity	minor
Message format string	The *$tmnxSmRunExtAuthType$* operation failed with a min delay violation error: Mindelay = *$tmnxEhsHEntryMinDelay$* is greater than Mindelay Interval: *$tmnxEhsHEntryMinDelayInterval$*. The script policy " *$tmnxEhsHEntryScriptPlcyName$*" created by the owner "*$tmnx EhsHEntryScriptPlcyOwner$*" was executed with cli-user account " *$tmnxSmRunExtUserName$*".
Cause	The tmnxEhsDroppedByMinDelay is generated when two consecutive executions of script policy specified by this Ehs event handler entry occurs with in the time period specified by tmnxEhsHEntryMinDelay.
Effect	The value of tmnxEhsHEntryStatsErrMinDelay gets incremented. Execution of the script policy stops.
Recovery	No recovery is necessary.

71.35 tmnxEhsHandlerInvoked

Table 1464: tmnxEhsHandlerInvoked properties

Property name	Value
Application name	SYSTEM
Event ID	2069
Event name	tmnxEhsHandlerInvoked
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.70
Default severity	minor
Message format string	Ehs handler :" *$tmnxEhsHandlerName$*" with the description : "*$tmnx EhsHandlerDescription$*" was invoked by the cli-user account " *$tmnx SmRunExtUserName$*".
Cause	The tmnxEhsHandlerInvoked notification is generated when the log event for a particular application-id and event-id/event name invokes EHS and creates a run Entry.
Effect	EHS might create a run entry to execute scripts.
Recovery	No recovery is necessary.

71.36 tmnxFtpClientFailure

Table 1465: tmnxFtpClientFailure properties

Property name	Value
Application name	SYSTEM
Event ID	2034
Event name	tmnxFtpClientFailure
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.34
Default severity	minor
Message format string	Ftp client operation for destination *$tmnxFtpFailureDestAddress$* failed with error message *$tmnxFtpFailureMsg$*
Cause	A file transfer operation initiated by the FTP client failed.
Effect	N/A
Recovery	N/A

71.37 tmnxModuleMallocFailed

Table 1466: tmnxModuleMallocFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2010
Event name	tmnxModuleMallocFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.12
Default severity	major
Message format string	Memory allocation request for *$tmnxModuleMallocSize$* bytes from module *$tmnxMemoryModule$* failed
Cause	A request to allocate memory from a particular module failed because the memory module was short on memory and could not support the size that was requested.
Effect	N/A
Recovery	N/A

71.38 tmnxRedCpmActive

Table 1467: tmnxRedCpmActive properties

Property name	Value
Application name	SYSTEM
Event ID	2028
Event name	tmnxRedCpmActive
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.28
Default severity	critical
Message format string	New active CPM card *$cpmSlotName$* is ready to accept CLI configuration commands and SNMP SET requests.
Cause	Following a redundancy switchover the new active CPM has completed its audit and is ready to accept management commands via CLI or SNMP SET requests.

Property name	Value
Effect	N/A
Recovery	N/A

71.39 tmnxRedSingleCpm

Table 1468: tmnxRedSingleCpm properties

Property name	Value
Application name	SYSTEM
Event ID	2029
Event name	tmnxRedSingleCpm
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.29
Default severity	critical
Message format string	The active CPM card *$cpmSlotName$* is operating in singleton mode. There is no standby CPM card.
Cause	In a system with a chassis with two CPM slots the active CPM could not detect a standby CPM in the chassis. When the operating state of TIMETRA-CHASSIS-MIB::tmnxCpmCardRedundant for the active CPM card transitions to a value of 'singleton (1)', this event is generated. When the active CPM later detects a standby CPM in the chassis, the ssiRedStandbySyncing event will be generated followed by a ssiRed StandbyReady event to indicate clearing of the CPM singleton state. The value of tmnxCpmCardRedundant will then transition to 'redundant Active (2)'."
Effect	N/A
Recovery	N/A

71.40 tmnxRedStandbyReady

Table 1469: tmnxRedStandbyReady properties

Property name	Value
Application name	SYSTEM
Event ID	2025

Property name	Value
Event name	tmnxRedStandbyReady
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.25
Default severity	major
Message format string	Redundancy synchronization with standby CPM card *$cpmSlotName$* has completed. Standby CPM is ready.
Cause	The synchronization of redundancy information onto the standby CPM has completed.
Effect	The standby CPM is now ready to take over control of the system if the active CPM fails or a manual switchover command is issued.
Recovery	N/A

71.41 tmnxRedStandbySyncing

Table 1470: tmnxRedStandbySyncing properties

Property name	Value
Application name	SYSTEM
Event ID	2024
Event name	tmnxRedStandbySyncing
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.24
Default severity	major
Message format string	Redundancy synchronization with standby CPM card *$cpmSlotName$* is in progress.
Cause	Synchronization of redundancy information onto the standby CPM was started. tmnxChassisNotifyHwIndex identifies the standby CPM.
Effect	N/A
Recovery	N/A

71.42 tmnxRedStandbySyncLost

Table 1471: tmnxRedStandbySyncLost properties

Property name	Value
Application name	SYSTEM
Event ID	2026
Event name	tmnxRedStandbySyncLost
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.26
Default severity	critical
Message format string	Redundancy synchronization with standby CPM card *$cpmSlotName$* has been lost.
Cause	The active CPM lost communitcation with the standby CPM.
Effect	N/A
Recovery	N/A

71.43 tmnxRedSwitchover

Table 1472: tmnxRedSwitchover properties

Property name	Value
Application name	SYSTEM
Event ID	2027
Event name	tmnxRedSwitchover
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.27
Default severity	critical
Message format string	Redundancy switchover from CPM card *$cpmSlotName$* because *$ssiRedFailoverReason$*.
Cause	The standby CPM detected that the active CPM has failed.
Effect	The standby CPM prepared to take over as the new active CPM.
Recovery	N/A

71.44 tmnxSmLaunchStartFailed

Table 1473: tmnxSmLaunchStartFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2068
Event name	tmnxSmLaunchStartFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.69
Default severity	minor
Message format string	Launch of *$tmnxSmRunExtAuthType$* operation failed with a error: *$smLaunchError$*. The script policy "*$tmnxEhsHEntryScriptPlcyName $*" created by the owner " *$tmnxEhsHEntryScriptPlcyOwner$*" was executed with cli-user account " *$tmnxSmRunExtUserName$*"
Cause	The tmnxSmLaunchStartFailed notification is generated when the launch start fails because : 1. The values of smLaunchScriptOwner and smLaunchScriptName don't have a existing entry in the smScriptTable. 2. The value of smScriptOperStatus is not 'enabled'. 3. The smScript Source value is NULL. 4. The value of smLaunchOperStatus object in smLaunchTable is not 'enabled'. 5. The check to see if the run Index is already in use fails. 6. The number of currently executing scripts invoked from this smLaunchTable entry is greater than smLaunchMax Running.
Effect	The result is indicated by incrementing the value of tmnxEhsHEntry StatsErrLaunch.
Recovery	No recovery is necessary.

71.45 tmnxSnmpdStateChange

Table 1474: tmnxSnmpdStateChange properties

Property name	Value
Application name	SYSTEM
Event ID	2023
Event name	tmnxSnmpdStateChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.23
Default severity	major

Property name	Value
Message format string	The SNMP agent has changed state. Administrative state is *$sbi SnmpdAdminStatus$* and operational state is *$sbiSnmpdOperStatus$*.
Cause	There was a change in either the adminstrative or operational state of the SNMP agent.
Effect	N/A
Recovery	N/A

71.46 tmnxSntpOperChange

Table 1475: tmnxSntpOperChange properties

Property name	Value
Application name	SYSTEM
Event ID	2032
Event name	tmnxSntpOperChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.32
Default severity	major
Message format string	SNTP's operational status is *$sntpOperStatus$*
Cause	There was a change in the operational state of SNTP.
Effect	N/A
Recovery	N/A

71.47 tmnxSssiMismatch

Table 1476: tmnxSssiMismatch properties

Property name	Value
Application name	SYSTEM
Event ID	2022
Event name	tmnxSssiMismatch
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.22

Property name	Value
Default severity	major
Message format string	Synchronization between CPMs is disabled therefore persistent SNMP index files may not be in sync
Cause	In a system with redundant CPM cards, upon completion of the bootup configuration synchronization was 'disabled' but the boot options file (bof) specifies the system is to be booted with persistent SNMP indexes.
Effect	Boot environment files are not synchronized. Following a system failover, SNMP indexes may not have the same values.
Recovery	Enable synchronization.

71.48 tmnxStateChange

Table 1477: tmnxStateChange properties

Property name	Value
Application name	SYSTEM
Event ID	2009
Event name	tmnxStateChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.11
Default severity	warning
Message format string	Status of *$tmnxNotifyObjectName$* changed administrative state: *$tmnxNotifyRowAdminState$*, operational state: *$tmnxNotifyRowOperState$*
Cause	A change occurred in either the adminstrative or operational state of a MIB table entry.
Effect	N/A
Recovery	No recovery is necessary.

71.49 tmnxSysAppStats24HrsAvailable

Table 1478: tmnxSysAppStats24HrsAvailable properties

Property name	Value
Application name	SYSTEM
Event ID	2071
Event name	tmnxSysAppStats24HrsAvailable
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.72
Default severity	warning
Message format string	New rows are available in the tmnxSysAppStats24HrsTable containing values collected at *$tmnxSysNotifAppStatsTime$* for application *$tmnxSysNotifAppStatsApplication$* type *$tmnxSysNotifAppStatsType$*
Cause	The system generates the tmnxSysAppStats24HrsAvailable notification when new rows are available in the tmnxSysAppStats24HrsTable. The value of tmnxSysNotifAppStatsTime indicates the time the system collected the values in the new rows. A non-zero value of tmnxSysNotifAppStatsApplication indicates the application; a zero value of tmnxSysNotifAppStatsApplication indicates that new values are available for all active applications. A non-zero value of tmnxSysNotifAppStatsType indicates the type of statistics; a zero value of tmnxSysNotifAppStatsType indicates that new values are available for all active types.
Effect	None.
Recovery	No recovery is necessary.

71.50 tmnxSysAppStatsWeekAvailable

Table 1479: tmnxSysAppStatsWeekAvailable properties

Property name	Value
Application name	SYSTEM
Event ID	2072
Event name	tmnxSysAppStatsWeekAvailable
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.73
Default severity	warning

Property name	Value
Message format string	New rows are available in the tmnxSysAppStatsWeekTable containing values collected at *$tmnxSysNotifAppStatsTime$*
Cause	The system generates the tmnxSysAppStatsWeekAvailable notification when new rows are available in the tmnxSysAppStatsWeekTable. The value of tmnxSysNotifAppStatsTime indicates the time the system collected the values in the new rows.
Effect	None.
Recovery	No recovery is necessary.

71.51 tmnxSysBaseMacAddressNotSet

Table 1480: tmnxSysBaseMacAddressNotSet properties

Property name	Value
Application name	SYSTEM
Event ID	2067
Event name	tmnxSysBaseMacAddressNotSet
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.68
Default severity	major
Message format string	System base MAC address is not set. Using generated value of *$tmnx ChassisBaseMacAddress$* which may not be unique.
Cause	The tmnxSysBaseMacAddressNotSet notification is generated once after the system boots up and the value of sbiSystemBaseMacAddress is all zeroes.
Effect	The system software is using the base MAC address specified in tmnx ChassisBaseMacAddress which may not be unique.
Recovery	Configure sbiSystemBaseMacAddress to a value other than all zeroes.

71.52 tmnxSysExecFinished

Table 1481: tmnxSysExecFinished properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2053
Event name	tmnxSysExecFinished
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.53
Default severity	major
Message format string	Possible messages: • The CLI user initiated '*$tmnxLogExecRollbackOpType$*' operation to process the commands in the SROS CLI file *$tmnxSysExecScript$* has completed with the result of *$tmnxSysExecResult$* • Processing of '*$tmnxLogExecRollbackOpType$*' configuration messages has completed with the result of *$tmnxSysExecResult$*
Cause	The tmnxSysExecFinished notification is generated upon the completion of the execution of a CLI command file or execution of 'vsd' configuration messages is completed. The value of tmnxSysExecScript indicates the command file when the value of tmnxLogExecRollback OpType is 'exec' or an empty string when the value of tmnxLogExec RollbackOpType is 'vsd'. The value of tmnxLogExecRollbackOpIndex indicates the row entry in TIMETRA-LOG-MIB::tmnxLogExecRollback OpTable for this CLI 'exec' or 'vsd' operation.
Effect	The effect is that the entry for the specified tmnxLogExecRollback OpIndex won't be updated, and no further notifications will be added to the specified index in the logger.
Recovery	When the value of tmnxSysExecResult is 'none' or 'success', no recovery is required. When the value is 'fail', the system may be left in an inconsistent state and the user should try to determine the reason for the failure. The user can attempt a recovery by manually entering CLI commands to reverse the failed configuration. The user can attempt a recovery by performing a rollback revert to a known good checkpoint. The user can attempt a recovery by rebooting the system with the bof pointing to a saved configuration file."

71.53 tmnxSysExecStarted

Table 1482: tmnxSysExecStarted properties

Property name	Value
Application name	SYSTEM
Event ID	2052
Event name	tmnxSysExecStarted

Property name	Value
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.52
Default severity	major
Message format string	Possible messages: • A CLI user has initiated an '*$tmnxLogExecRollbackOpType$*' operation to process the commands in the SROS CLI file *$tmnxSysExecScript$* • Processing of '*$tmnxLogExecRollbackOpType$*' configuration messages has been iniitated
Cause	The tmnxSysExecStarted notification is generated when the user initiates a CLI 'exec' operation to process a file of SROS CLI commands or processing of 'vsd' configuration messages have been initiated. The value of tmnxSysExecScript indicates the command file when the value of tmnxLogExecRollbackOpType is 'exec' or an empty string when the value of tmnxLogExecRollbackOpType is 'vsd'. The value of tmnxLogExecRollbackOpIndex indicates the row entry in TIMETRA-LOG-MIB::tmnxLogExecRollbackOpTable for this CLI 'exec' or 'vsd' operation.
Effect	All change notifications generated after the generation of this notification and before the tmnxSysExecFinished will be logged in the TIMETRA-LOG-MIB::tmnxLogExecRollbackEventEntry. Once the tmnx SysExecFinished notification is triggered, a Network Management System (NMS) is able to walk the aforementioned log table to retrieve the list of all objects that have been modified during this transaction.
Recovery	There is no recovery required for this notification.

71.54 tmnxSysNvsysFileError

Table 1483: tmnxSysNvsysFileError properties

Property name	Value
Application name	SYSTEM
Event ID	2056
Event name	tmnxSysNvsysFileError
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.56
Default severity	minor
Message format string	Failure to *$tmnxSysFileErrorType$* file *$fileName$*

Property name	Value
Cause	The tmnxSysNvsysFileError notification is generated when there is a failure in accessing the nvsys file as specified by tmnxSysFileError Type.
Effect	The specified nvsys file operation is unsuccessful.
Recovery	The user should investigate why the failure occurred. A failure can indicate a problem with the compact flash.

71.55 tmnxSysRollbackDeleteStarted

Table 1484: tmnxSysRollbackDeleteStarted properties

Property name	Value
Application name	SYSTEM
Event ID	2055
Event name	tmnxSysRollbackDeleteStarted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.55
Default severity	minor
Message format string	Rollback delete of file *$fileName$* started
Cause	The tmnxSysRollbackDeleteStarted notification is generated when the user initiates a rollback delete as specified by by tmnxSysRollback Index and tmnxSysRollbackFileType.
Effect	The specified configuration file is deleted.
Recovery	There is no recovery required for this notification.

71.56 tmnxSysRollbackFileDeleteStatus

Table 1485: tmnxSysRollbackFileDeleteStatus properties

Property name	Value
Application name	SYSTEM
Event ID	2045
Event name	tmnxSysRollbackFileDeleteStatus

Property name	Value
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.45
Default severity	minor
Message format string	Rollback deletion of file *$fileName$ $result$*
Cause	The tmnxSysRollbackFileDeleteStatus notification is generated upon the completion of a rollback file delete as specified by tmnxSysRollback Index and tmnxSysRollbackFileType.
Effect	The result is indicated by the value of tmnxSysRollbackFileDelete Result.
Recovery	When the value of tmnxSysRollbackFileDeleteResult is none, in Progress or success no recovery is required. When the value is failed, the user should try to determine the reason for the failure. The user can attempt a recovery by deleting the file again.

71.57 tmnxSysRollbackSaveStarted

Table 1486: tmnxSysRollbackSaveStarted properties

Property name	Value
Application name	SYSTEM
Event ID	2054
Event name	tmnxSysRollbackSaveStarted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.54
Default severity	minor
Message format string	Rollback save of file *$fileName$* started
Cause	The tmnxSysRollbackSaveStarted notification is generated when the user initiates a rollback save as specified by tmnxSysRollbackFileType.
Effect	The specified configuration file is saved.
Recovery	There is no recovery required for this notification.

71.58 tmnxSysRollbackSaveStatusChange

Table 1487: tmnxSysRollbackSaveStatusChange properties

Property name	Value
Application name	SYSTEM
Event ID	2044
Event name	tmnxSysRollbackSaveStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.44
Default severity	major
Message format string	Rollback save of file *$fileName$ $result$*
Cause	The tmnxSysRollbackSaveStatusChange notification is generated upon the completion of a rollback save as specified by tmnxSysRollbackFile Type.
Effect	The result is indicated by value of tmnxSysRollbackSaveResult.
Recovery	When the value of tmnxSysRollbackSaveResult is none, inProgress or success no recovery is required. When the value is is failed, the user should try to determine the reason for the failure. The user can attempt a recovery by attempting the rollback save again.

71.59 tmnxSysRollbackStarted

Table 1488: tmnxSysRollbackStarted properties

Property name	Value
Application name	SYSTEM
Event ID	2042
Event name	tmnxSysRollbackStarted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.42
Default severity	major
Message format string	Rollback revert of file *$fileName$* started
Cause	The tmnxSysRollbackStarted notification is generated when the user initiates a revert of the rollback checkpoint file specified by tmnxSys RollbackIndex and tmnxSysRollbackFileType.
Effect	The specified file is executed and system configuration may change.

Property name	Value
Recovery	There is no recovery required for this notification.

71.60 tmnxSysRollbackStatusChange

Table 1489: tmnxSysRollbackStatusChange properties

Property name	Value
Application name	SYSTEM
Event ID	2043
Event name	tmnxSysRollbackStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.43
Default severity	critical
Message format string	Rollback revert of file *$fileName$ $result$*
Cause	The tmnxSysRollbackStatusChange notification is generated upon the completion of a rollback revert as specified by tmnxSysRollbackIndex and tmnxSysRollbackFileType.
Effect	The result is indicated by the value of tmnxSysRollbackResult.
Recovery	When the value of tmnxSysRollbackResult is none, inProgress or success no recovery is required. When the value is failed, the user should try to determine the reason for the failure. The user can attempt a recovery by reverting back to a known good checkpoint. The user may reboot the system with the bof pointing to a saved configuration file.

71.61 tmnxSysVsdServerAvailable

Table 1490: tmnxSysVsdServerAvailable properties

Property name	Value
Application name	SYSTEM
Event ID	2063
Event name	tmnxSysVsdServerAvailable
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.63

Property name	Value
Default severity	minor
Message format string	VSD server *$tmnxSysNotifVsdServerName$* is available
Cause	The tmnxSysVsdServerAvailable notification is generated when system discover a new VSD server.
Effect	System will use this information to establish communication with new VSD server as needed.
Recovery	None needed.

71.62 tmnxSysVsdServerUnavailable

Table 1491: tmnxSysVsdServerUnavailable properties

Property name	Value
Application name	SYSTEM
Event ID	2064
Event name	tmnxSysVsdServerUnavailable
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.64
Default severity	minor
Message format string	VSD server *$tmnxSysNotifVsdServerName$* is unavailable
Cause	The tmnxSysVsdServerAvailable notification is generated when system loses connection to VSD.
Effect	System will use this information and stop communication with this VSD server as needed.
Recovery	None needed.

71.63 tmnxSysXmppServerFunctional

Table 1492: tmnxSysXmppServerFunctional properties

Property name	Value
Application name	SYSTEM
Event ID	2065

Property name	Value
Event name	tmnxSysXmppServerFunctional
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.65
Default severity	minor
Message format string	XMPP server *$tmnxSysNotifXmppServerName$* is functional
Cause	The tmnxSysXmppServerFunctional notification is generated when system discover a new XMPP server.
Effect	System will use this information to establish communication with new XMPP server as needed.
Recovery	None needed.

71.64 tmnxSysXmppServerNotFunctional

Table 1493: tmnxSysXmppServerNotFunctional properties

Property name	Value
Application name	SYSTEM
Event ID	2066
Event name	tmnxSysXmppServerNotFunctional
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.66
Default severity	minor
Message format string	XMPP server *$tmnxSysNotifXmppServerName$* is not functional
Cause	The tmnxSysXmppServerNotFunctional notification is generated when system can not communicate with XMPP server.
Effect	Communication with XMPP server will stop.
Recovery	Check to see why XMPP server has stopped communicatinng.

71.65 tmnxTrapDropped

Table 1494: tmnxTrapDropped properties

Property name	Value
Application name	SYSTEM
Event ID	2011
Event name	tmnxTrapDropped
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.13
Default severity	major
Message format string	Dropped notification *$tmnxDroppedTrapName$* for *$tmnxDroppedTrapEntryName$* because of *$tmnxTrapDroppedReasonCode$* - *$tmnxTrapDroppedCount$* traps dropped
Cause	A tmnxTrapDropped notification is generated when a trap is dropped for the reason specified by the reason code. The tmnxTrapDroppedEntryID identifies the table entry associated with the dropped trap. A nonzero value of the object tmnxTrapDroppedCount indicates the number of traps dropped for the current flow of traps, identified by the values of tmnxDroppedTrapID, tmnxTrapDroppedReasonCode and tmnxTrapDroppedEntryID.
Effect	N/A
Recovery	N/A

72 TLS

72.1 tmnxTlsFailure

Table 1495: tmnxTlsFailure properties

Property name	Value
Application name	TLS
Event ID	2003
Event name	tmnxTlsFailure
SNMP notification prefix and OID	TIMETRA-TLS-MIB.tmnxTlsNotifications.3
Default severity	minor
Message format string	TLS session failure for application *$tmnxTlsAppId$ $tmnxTlsRole$* router instance *$tmnxTlsVRtrID$* source address *$tmnxTlsLocalAddr$* sourcePort *$tmnxTlsLocalPort$* destination address *$tmnxTlsRemote Addr$* destinationPort *$tmnxTlsRemotePort$* failure reason *$tmnxTls FailureReason$*
Cause	The tmnxTlsFailure notification is generated when an error occurred in a TLS session. The tmnxTlsFailureReason specifies the kind of error.
Effect	The TLS session is terminated.
Recovery	Corrective action should be taken based on the failure reason indicated by tmnxTlsFailureReason.

72.2 tmnxTlsInitiateSession

Table 1496: tmnxTlsInitiateSession properties

Property name	Value
Application name	TLS
Event ID	2001
Event name	tmnxTlsInitiateSession
SNMP notification prefix and OID	TIMETRA-TLS-MIB.tmnxTlsNotifications.1

Property name	Value
Default severity	minor
Message format string	TLS session initiated for application *$tmnxTlsAppId$ $tmnxTlsRole $* router instance *$tmnxTlsVRtrID$* source address *$tmnxTlsLocal Addr$* sourcePort *$tmnxTlsLocalPort$* destination address *$tmnxTls RemoteAddr$* destinationPort *$tmnxTlsRemotePort$* tls state *$tmnxTls ConnectionState$*
Cause	The tmnxTlsInitiateSession notification is generated when an attempt to create a TLS session is made. The value connected of leaf tmnxTls ConnectionState indicates the TLS session is successfully created.
Effect	The TLS session is going to be created or it was created.
Recovery	No recovery actions are needed.

72.3 tmnxTlsTermination

Table 1497: tmnxTlsTermination properties

Property name	Value
Application name	TLS
Event ID	2002
Event name	tmnxTlsTermination
SNMP notification prefix and OID	TIMETRA-TLS-MIB.tmnxTlsNotifications.2
Default severity	minor
Message format string	TLS session terminated for application *$tmnxTlsAppId$ $tmnxTlsRole $* router instance *$tmnxTlsVRtrID$* source address *$tmnxTlsLocalAddr $* sourcePort *$tmnxTlsLocalPort$* destination address *$tmnxTlsRemote Addr$* destinationPort *$tmnxTlsRemotePort$*
Cause	The tmnxTlsTermination notifications is generated when a TLS session is normally terminated. If the session is terminated because of a failure tmnxTlsFailure notification is generated instead.
Effect	The TLS session is terminated.
Recovery	No recovery actions are needed.

73 USER

73.1 cli_config_io

Table 1498: cli_config_io properties

Property name	Value
Application name	USER
Event ID	2011
Event name	cli_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	A CLI command was entered in a configuration node
Effect	The configuration was changed by the CLI command.
Recovery	No recovery is required

73.2 cli_unauth_config_io

Table 1499: cli_unauth_config_io properties

Property name	Value
Application name	USER
Event ID	2013
Event name	cli_unauth_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	User has entered configuration command for which he is not authorized.

Property name	Value
Effect	The CLI command was not processed.
Recovery	No recovery is required.

73.3 cli_unauth_user_io

Table 1500: cli_unauth_user_io properties

Property name	Value
Application name	USER
Event ID	2012
Event name	cli_unauth_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	User has entered command for which he is not authorized.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

73.4 cli_user_io

Table 1501: cli_user_io properties

Property name	Value
Application name	USER
Event ID	2009
Event name	cli_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	A CLI command was entered.

Property name	Value
Effect	The CLI command was processed.
Recovery	No recovery is required.

73.5 cli_user_login

Table 1502: cli_user_login properties

Property name	Value
Application name	USER
Event ID	2001
Event name	cli_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$* logged in
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required.

73.6 cli_user_login_failed

Table 1503: cli_user_login_failed properties

Property name	Value
Application name	USER
Event ID	2003
Event name	cli_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$* failed authentication
Cause	A user failed authentication.

Property name	Value
Effect	The user access session was not started. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

73.7 cli_user_login_max_attempts

Table 1504: cli_user_login_max_attempts properties

Property name	Value
Application name	USER
Event ID	2004
Event name	cli_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in, user is locked out
Cause	A user failed to authenticate in more than the permitted number of retries.
Effect	If telnet the session terminates; console no effect
Recovery	No recovery is required.

73.8 cli_user_logout

Table 1505: cli_user_logout properties

Property name	Value
Application name	USER
Event ID	2002
Event name	cli_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Message format string	User from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

73.9 ftp_user_login

Table 1506: ftp_user_login properties

Property name	Value
Application name	USER
Event ID	2005
Event name	ftp_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	FTP user from *$srcAddr$* logged in
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required

73.10 ftp_user_login_failed

Table 1507: ftp_user_login_failed properties

Property name	Value
Application name	USER
Event ID	2007
Event name	ftp_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Message format string	FTP user from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session was not started. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

73.11 ftp_user_login_max_attempts

Table 1508: ftp_user_login_max_attempts properties

Property name	Value
Application name	USER
Event ID	2008
Event name	ftp_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in, user is locked out
Cause	A user failed to authenticate in more than the permitted number of retries.
Effect	The ftp session was terminated.
Recovery	No recovery is required.

73.12 ftp_user_logout

Table 1509: ftp_user_logout properties

Property name	Value
Application name	USER
Event ID	2006
Event name	ftp_user_logout

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	FTP user from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

73.13 grpc_config_io

Table 1510: grpc_config_io properties

Property name	Value
Application name	USER
Event ID	2031
Event name	grpc_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$mdcliString$* xpath = *$xpathString$*
Cause	A gRPC request to change configuration data was received.
Effect	The configuration was changed by the gRPC request.
Recovery	No recovery is required

73.14 grpc_unauth_config_io

Table 1511: grpc_unauth_config_io properties

Property name	Value
Application name	USER
Event ID	2033

Property name	Value
Event name	grpc_unauth_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$mdcliString$* xpath = *$xpathString$*
Cause	User made a gRPC request to change configuration data for which he is not authorized.
Effect	The gRPC request was not processed.
Recovery	No recovery is required.

73.15 grpc_unauth_user_io

Table 1512: grpc_unauth_user_io properties

Property name	Value
Application name	USER
Event ID	2032
Event name	grpc_unauth_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$mdcliString$* xpath = *$xpathString$*
Cause	User made a gRPC request for which he is not authorized.
Effect	The gRPC request was not processed.
Recovery	No recovery is required.

73.16 grpc_user_io

Table 1513: grpc_user_io properties

Property name	Value
Application name	USER
Event ID	2030
Event name	grpc_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$mdcliString$* xpath = *$xpathString$*
Cause	A gRPC request was received.
Effect	The gRPC request was processed.
Recovery	No recovery is required.

73.17 mct_user_login

Table 1514: mct_user_login properties

Property name	Value
Application name	USER
Event ID	2016
Event name	mct_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User from *$srcAddr$* logged in
Cause	A user successfully authenticated for login via MCT.
Effect	A user access session was started.
Recovery	No recovery is required.

73.18 mct_user_login_failed

Table 1515: mct_user_login_failed properties

Property name	Value
Application name	USER
Event ID	2014
Event name	mct_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session was not started. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

73.19 mct_user_login_max_attempts

Table 1516: mct_user_login_max_attempts properties

Property name	Value
Application name	USER
Event ID	2015
Event name	mct_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in
Cause	A user failed to authenticate in more than the permitted number of retries.
Effect	No effect.
Recovery	No recovery is required.

73.20 mct_user_logout

Table 1517: mct_user_logout properties

Property name	Value
Application name	USER
Event ID	2017
Event name	mct_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	MCT User from *$srcAddr$* logged out
Cause	A user logged out from MCT.
Effect	The user access session ended.
Recovery	No recovery is required.

73.21 md_cli_config_io

Table 1518: md_cli_config_io properties

Property name	Value
Application name	USER
Event ID	2023
Event name	md_cli_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$mdcliString$* xpath = *$xpathString$*
Cause	A CLI command was entered in a configuration node in the MD-CLI engine.
Effect	The configuration was changed by the CLI command in the MD-CLI engine.
Recovery	No recovery is required

73.22 md_cli_unauth_config_io

Table 1519: md_cli_unauth_config_io properties

Property name	Value
Application name	USER
Event ID	2025
Event name	md_cli_unauth_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$mdcliString$* xpath = *$xpathString$*
Cause	User has entered configuration command for which he is not authorized.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

73.23 md_cli_unauth_user_io

Table 1520: md_cli_unauth_user_io properties

Property name	Value
Application name	USER
Event ID	2024
Event name	md_cli_unauth_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$mdcliString$* xpath = *$xpathString$*
Cause	User has entered command for which he is not authorized.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

73.24 md_cli_user_io

Table 1521: md_cli_user_io properties

Property name	Value
Application name	USER
Event ID	2022
Event name	md_cli_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$mdcliString$* xpath = *$xpathString$*
Cause	A CLI command was entered in the MD-CLI engine.
Effect	The CLI command was processed in the MD-CLI engine.
Recovery	No recovery is required.

73.25 netconf_config_io

Table 1522: netconf_config_io properties

Property name	Value
Application name	USER
Event ID	2027
Event name	netconf_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$mdcliString$* xpath = *$xpathString$*
Cause	A Netconf request to change configuration data was received.
Effect	The configuration was changed by the Netconf request.
Recovery	No recovery is required

73.26 netconf_unauth_config_io

Table 1523: netconf_unauth_config_io properties

Property name	Value
Application name	USER
Event ID	2029
Event name	netconf_unauth_config_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$mdcliString$* xpath = *$xpathString$*
Cause	User made a Netconf request to change configuration data for which he is not authorized.
Effect	The Netconf request was not processed.
Recovery	No recovery is required.

73.27 netconf_unauth_user_io

Table 1524: netconf_unauth_user_io properties

Property name	Value
Application name	USER
Event ID	2028
Event name	netconf_unauth_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*. *$message$*: *$mdcliString$* xpath = *$xpathString$*
Cause	User made a Netconf request for which he is not authorized.
Effect	The Netconf request was not processed.
Recovery	No recovery is required.

73.28 netconf_user_io

Table 1525: netconf_user_io properties

Property name	Value
Application name	USER
Event ID	2026
Event name	netconf_user_io
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$*: *$mdcliString$* xpath = *$xpathString$*
Cause	A Netconf request was received.
Effect	The Netconf request was processed.
Recovery	No recovery is required.

73.29 netconf_user_login

Table 1526: netconf_user_login properties

Property name	Value
Application name	USER
Event ID	2018
Event name	netconf_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Netconf user from *$srcAddr$* logged in
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required.

73.30 netconf_user_login_failed

Table 1527: netconf_user_login_failed properties

Property name	Value
Application name	USER
Event ID	2020
Event name	netconf_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Netconf user from *$srcAddr$* failed authentication
Cause	A user failed authentication.
Effect	The user access session was not started. The user is given another opportunity to authenticate himself.
Recovery	No recovery is required.

73.31 netconf_user_login_max_attempts

Table 1528: netconf_user_login_max_attempts properties

Property name	Value
Application name	USER
Event ID	2021
Event name	netconf_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in, user is locked out
Cause	A user failed to authenticate in more than the permitted number of retries.
Effect	The netconf session was terminated.
Recovery	No recovery is required.

73.32 netconf_user_logout

Table 1529: netconf_user_logout properties

Property name	Value
Application name	USER
Event ID	2019
Event name	netconf_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Netconf user from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

73.33 snmp_user_set

Table 1530: snmp_user_set properties

Property name	Value
Application name	USER
Event ID	2010
Event name	snmp_user_set
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	SNMP user from *$srcAddr$*> *$vbList$*
Cause	An SNMP SET reqest was received.
Effect	Configuration was changed by an SNMP SET operation.
Recovery	No recovery is required.

74 VIDEO

74.1 tmnxVdoAdSpliceAbort

Table 1531: tmnxVdoAdSpliceAbort properties

Property name	Value
Application name	VIDEO
Event ID	2006
Event name	tmnxVdoAdSpliceAbort
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.6
Default severity	warning
Message format string	An ad splice operation has been aborted - Service Id - *$tmnxVdo NotifysvcId$*, Video interface - *$tmnxVdoNotifyIfName$*, Group address - *$tmnxVdoNotifyGroupAddress$*, Source address - *$tmnxVdoNotify SourceAddress$*, Session Id - *$tmnxVdoNotifyAdSpliceSessionId$*, Abort time - *$tmnxVdoNotifyAdSpliceAbortTime$*, Duration - *$tmnx VdoNotifyAdSpliceDuration$*, Packets - *$tmnxVdoLogAdSplicePackets $*, Octets - *$tmnxVdoLogAdSpliceOctets$*, Bit rate - *$tmnxVdoLog AdSpliceBitRate$* Kbps
Cause	This event will be generated when an ad splice is aborted.
Effect	N/A
Recovery	N/A

74.2 tmnxVdoClientSessionsLmtCleared

Table 1532: tmnxVdoClientSessionsLmtCleared properties

Property name	Value
Application name	VIDEO
Event ID	2008
Event name	tmnxVdoClientSessionsLmtCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.8

Property name	Value
Default severity	warning
Message format string	Number of RTCP sessions back to the limit for client *$tmnxVdoNotify ClientAddress$*
Cause	N/A
Effect	N/A
Recovery	N/A

74.3 tmnxVdoClientSessionsLmtExceeded

Table 1533: tmnxVdoClientSessionsLmtExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2007
Event name	tmnxVdoClientSessionsLmtExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.7
Default severity	warning
Message format string	Threshold for number of RTCP sessions exceeded for client *$tmnxVdo NotifyClientAddress$*
Cause	N/A
Effect	N/A
Recovery	N/A

74.4 tmnxVdoDuplicateSsrcId

Table 1534: tmnxVdoDuplicateSsrcId properties

Property name	Value
Application name	VIDEO
Event ID	2001
Event name	tmnxVdoDuplicateSsrcId

Property name	Value
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.1
Default severity	warning
Message format string	Duplicate SSRC Id *$tmnxVdoGrpSrcSSRCId$* detected: Service Id - *$svcId$*, Video interface - *$tmnxVdoIfName$*, Group address - *$tmnx VdoGrpSrcGroupAddress$*, Source address - *$tmnxVdoGrpSrcSource Address$*
Cause	This event will be generated for a video channel when we notice that it has an SSRC that conflicts with another SG's SSRC.
Effect	N/A
Recovery	The only way to clear this is by clearing one of the channels having the duplicate SSRC.

74.5 tmnxVdoGrpSrcAnlyzrErrState

Table 1535: tmnxVdoGrpSrcAnlyzrErrState properties

Property name	Value
Application name	VIDEO
Event ID	2009
Event name	tmnxVdoGrpSrcAnlyzrErrState
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.9
Default severity	warning
Message format string	Last 10 seconds analyzer state for - Service Id - *$tmnxVdoNotifysvcId $*, Video interface - *$tmnxVdoNotifyIfName$*, Group address - *$tmnx VdoNotifyGroupAddress$*, Source address - *$tmnxVdoNotifySource Address$* is *$tmnxVdoNotifyAnalyzerState$*
Cause	The tmnxVdoGrpSrcAnlyzrErrState notification is raised whenever a video channel analyzer's error state changes to one of these values - TNC (Tech Non-Conformance), QOS (Quality of Service), POA (Program off Air).
Effect	This trap is informational. No effects are caused by this trap.
Recovery	No recovery mechanism is required.

74.6 tmnxVdoGrpSrcAnlyzrStClear

Table 1536: tmnxVdoGrpSrcAnlyzrStClear properties

Property name	Value
Application name	VIDEO
Event ID	2010
Event name	tmnxVdoGrpSrcAnlyzrStClear
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.10
Default severity	warning
Message format string	Analyzer state is cleared for - Service Id - *$tmnxVdoNotifysvcId$*, Video interface - *$tmnxVdoNotifyIfName$*, Group address - *$tmnxVdoNotify GroupAddress$*, Source address - *$tmnxVdoNotifySourceAddress$*
Cause	The tmnxVdoGrpSrcAnlyzrStClear notification is raised whenever a video channel analyzer's error state has recovered from past errors and is good for the last 10 seconds.
Effect	This trap is informational. No effects are caused by this trap.
Recovery	No recovery mechanism is required.

74.7 tmnxVdoMdaSessionsLimitCleared

Table 1537: tmnxVdoMdaSessionsLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2004
Event name	tmnxVdoMdaSessionsLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.4
Default severity	warning
Message format string	Number of RTCP sessions back to the limit - *$tmnxVdoGrpMdaActive RtcpSessions$* sessions active on MDA *$tmnxChassisIndex$*/ *$tmnx CardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	This event will be generated for a video MDA when the number of active RTCP sessions are back to with in the limit.
Effect	N/A

Property name	Value
Recovery	N/A

74.8 tmnxVdoMdaSessionsLimitExceeded

Table 1538: tmnxVdoMdaSessionsLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2002
Event name	tmnxVdoMdaSessionsLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.2
Default severity	warning
Message format string	Threshold for number of RTCP sessions exceeded - *$tmnxVdoGrpMdaActiveRtcpSessions$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	This event will be generated for a video MDA when we exceed supported max sessions.
Effect	N/A
Recovery	N/A

74.9 tmnxVdoMdaSGLimitCleared

Table 1539: tmnxVdoMdaSGLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2005
Event name	tmnxVdoMdaSGLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.5
Default severity	warning

Property name	Value
Message format string	Number of channels back to the limit - *$tmnxVdoGrpMdaChannels$* channels active on MDA *$tmnxChassisIndex$*/ *$tmnxCardSlotNum$*/ *$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	This event will be generated for a video MDA when the number of channels are back to with in the limit.
Effect	N/A
Recovery	N/A

74.10 tmnxVdoMdaSGLimitExceeded

Table 1540: tmnxVdoMdaSGLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2003
Event name	tmnxVdoMdaSGLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.3
Default severity	warning
Message format string	Threshold for number of channels exceeded - *$tmnxVdoGrpMda Channels$* channels active on MDA *$tmnxChassisIndex$*/ *$tmnxCard SlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	This event will be generated for a video MDA when we exceed supported max channels.
Effect	N/A
Recovery	N/A

75 VRRP

75.1 tmnxVrrpBecameBackup

Table 1541: tmnxVrrpBecameBackup properties

Property name	Value
Application name	VRRP
Event ID	2006
Event name	tmnxVrrpBecameBackup
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.4
Default severity	minor
Message format string	VRRP virtual router instance *$vrrpOperVrId$* on interface *$ifIndex$* changed state to backup - current master is *$vrrpOperMasterIpAddr$*
Cause	The sending agent has transitioned to 'Backup' state.
Effect	N/A
Recovery	N/A

75.2 tmnxVrrpBfdIntfSessStateChgd

Table 1542: tmnxVrrpBfdIntfSessStateChgd properties

Property name	Value
Application name	VRRP
Event ID	2008
Event name	tmnxVrrpBfdIntfSessStateChgd
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.5
Default severity	minor
Message format string	BFD session on service *$tmnxVrrpNotifBfdIntfSvcId$* interface *$tmnx VrrpNotifBfdIntfIfName$* to peer *$tmnxVrrpNotifBfdIntfDestIp$* changed state to *$tmnxVrrpNotifBfdIntfSessState$*.

Property name	Value
Cause	The operational state of a BFD session of the VRRP instance changed.
Effect	N/A
Recovery	N/A

75.3 tmnxVrrpIPListMismatch

Table 1543: tmnxVrrpIPListMismatch properties

Property name	Value
Application name	VRRP
Event ID	2003
Event name	tmnxVrrpIPListMismatch
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.1
Default severity	minor
Message format string	IP Address list in VRRP advertisement from *$tmnxVrrpRouterMasterPrimaryAddr$* did not match address list configured for VRRP instance *$vrrpOperVrId$* on interface *$ifIndex$*
Cause	The IP address list in the advertisement messages received from the current master did not match the configured IP address list. This is an edge triggered event. A second event will not be generated for a packet from the same master until this event has been cleared.
Effect	N/A
Recovery	N/A

75.4 tmnxVrrpIPListMismatchClear

Table 1544: tmnxVrrpIPListMismatchClear properties

Property name	Value
Application name	VRRP
Event ID	2004
Event name	tmnxVrrpIPListMismatchClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.2
Default severity	minor
Message format string	Previously generated address list mismatch trap cleared for VRRP instance *$vrrpOperVrId$* on interface *$ifIndex$* for advertisements from *$tmnxVrrpRouterMasterPrimaryAddr$*
Cause	A previously ocurring tmnxVrrpIPListMismatch event has been cleared because the IP address list in the advertisement messages received from the current master now matches the configured IP address list. This is an edge triggered event. A second event will not be generated for a packet from the same master until this event has been set again.
Effect	N/A
Recovery	N/A

75.5 tmnxVrrpMultipleOwners

Table 1545: tmnxVrrpMultipleOwners properties

Property name	Value
Application name	VRRP
Event ID	2005
Event name	tmnxVrrpMultipleOwners
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.3
Default severity	minor
Message format string	*$tmnxVrrpRouterMasterPrimaryAddr$* is advertising itself as an owner for VRRP instance *$vrrpOperVrId$* which conflicts with owner instance on interface *$ifIndex$*
Cause	A VRRP virtual router instance that has been configured as an owner noticed that that another VRRP instance is also advertising itself as an owner.
Effect	N/A
Recovery	N/A

75.6 tmnxVrrpOperDownInvalidMac

Table 1546: tmnxVrrpOperDownInvalidMac properties

Property name	Value
Application name	VRRP
Event ID	2020
Event name	tmnxVrrpOperDownInvalidMac
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.15
Default severity	minor
Message format string	tmnxVrrpOperDownInvalidMac notification from VR *$vrrpOperVrId$* on interface *$ifIndex$*. VR is not allowed to be operational.
Cause	The tmnxVrrpOperDownInvalidMac is generated when the operational virtual MAC of an IPv4 VRRP instance conflicts with the MAC of the parent interface, or with the operational virtual MAC addresses of other VRRP instances under the same interface.
Effect	The VRRP virtual router instance is not allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification."

75.7 tmnxVrrpOperDownInvalidMacClear

Table 1547: tmnxVrrpOperDownInvalidMacClear properties

Property name	Value
Application name	VRRP
Event ID	2021
Event name	tmnxVrrpOperDownInvalidMacClear
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.16
Default severity	minor
Message format string	tmnxVrrpOperDownInvalidMac notification from VR *$vrrpOperVrId$* on interface *$ifIndex$* has been cleared.
Cause	The tmnxVrrpOperDownInvalidMacClear is generated when a previously occurring tmnxVrrpOperDownInvalidMac notification has been cleared. Operational virtual MAC of an IPv4 VRRP instance does not have any conflict with the MAC of the parent interface or with the

Property name	Value
	operational virtual MAC addresses of other VRRP instances under the same interface.
Effect	The VRRP virtual router instance is allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification."

75.8 tVrrpBecameBackup

Table 1548: tVrrpBecameBackup properties

Property name	Value
Application name	VRRP
Event ID	2010
Event name	tVrrpBecameBackup
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.6
Default severity	minor
Message format string	VRRP virtual router instance *$vrrpOperationsVrId$* on interface *$if Index$* changed state to backup - current master is *$vrrpOperations MasterIpAddr$*
Cause	The sending agent has transitioned to 'Backup' state.
Effect	N/A
Recovery	N/A

75.9 tVrrpIPListMismatch

Table 1549: tVrrpIPListMismatch properties

Property name	Value
Application name	VRRP
Event ID	2012
Event name	tVrrpIPListMismatch
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.8

Property name	Value
Default severity	minor
Message format string	IPv6 Address list in VRRP advertisement from *$tVrrpRtrMasterPrimaryAddr$* did not match address list configured for VRRP instance *$vrrpOperationsVrId$* on interface *$ifIndex$*
Cause	The IPv6 address list in the advertisement messages received from the current master did not match the configured IPv6 address list. This is an edge triggered event. A second event will not be generated for a packet from the same master until this event has been cleared.
Effect	N/A
Recovery	N/A

75.10 tVrrpIPListMismatchClear

Table 1550: tVrrpIPListMismatchClear properties

Property name	Value
Application name	VRRP
Event ID	2013
Event name	tVrrpIPListMismatchClear
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.9
Default severity	minor
Message format string	Previously generated address list mismatch trap cleared for VRRP instance *$vrrpOperationsVrId$* on interface *$ifIndex$* for advertisements from *$tVrrpRtrMasterPrimaryAddr$*
Cause	A previously ocurring tVrrpIPListMismatch event has been cleared because the IPv6 address list in the advertisement messages received from the current master now matches the configured IPv6 address list. This is an edge triggered event. A second event will not be generated for a packet from the same master until this event has been set again.
Effect	N/A
Recovery	N/A

75.11 tVrrpMultipleOwners

Table 1551: tVrrpMultipleOwners properties

Property name	Value
Application name	VRRP
Event ID	2014
Event name	tVrrpMultipleOwners
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.10
Default severity	minor
Message format string	*$tVrrpRtrMasterPrimaryAddr$* is advertising itself as an owner for VRRP instance *$vrrpOperationsVrId$* which conflicts with owner instance on interface *$ifIndex$*
Cause	A VRRP virtual router instance that has been configured as an owner noticed that another VRRP instance is also advertising itself as an owner.
Effect	N/A
Recovery	N/A

75.12 tVrrpOperDownInvalidMac

Table 1552: tVrrpOperDownInvalidMac properties

Property name	Value
Application name	VRRP
Event ID	2018
Event name	tVrrpOperDownInvalidMac
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.13
Default severity	minor
Message format string	tVrrpOperDownInvalidMac notification from IPv6 VR *$vrrpOperations VrId$* on interface *$ifIndex$*. VR is not allowed to be operational.
Cause	The tVrrpOperDownInvalidMac is generated when the operational virtual MAC of an IPv6 VRRP instance conflicts with the MAC of the parent interface, or with the operational virtual MAC addresses of other VRRP instances under the same interface.

Property name	Value
Effect	The VRRP virtual router instance is not allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification."

75.13 tVrrpOperDownInvalidMacClear

Table 1553: tVrrpOperDownInvalidMacClear properties

Property name	Value
Application name	VRRP
Event ID	2019
Event name	tVrrpOperDownInvalidMacClear
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.14
Default severity	minor
Message format string	tVrrpOperDownInvalidMac notification from IPv6 VR *$vrrpOperationsVrId$* on interface *$ifIndex$* has been cleared.
Cause	The tVrrpOperDownInvalidMacClear is generated when a previously occurring tVrrpOperDownInvalidMac notification has been cleared. Operational virtual MAC of an IPv6 VRRP instance does not have any conflict with the MAC of the parent interface or with the operational virtual MAC addresses of other VRRP instances under the same interface.
Effect	The VRRP virtual router instance is allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification."

75.14 tVrrpPacketDiscarded

Table 1554: tVrrpPacketDiscarded properties

Property name	Value
Application name	VRRP
Event ID	2015
Event name	tVrrpPacketDiscarded

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Discarded VRRP packet from *$vrrpPacketSrc$* because *$vrrpPacket DiscardReason$*
Cause	A VRRP packet we discarded. The following checks are performed on an incoming VRRP packet - verify that the IP TTL is 255. - verify the VRRP version - verify that the received packet length is greater than or equal to the VRRP header - verify the VRRP checksum - perform authentication specified by Auth Type If any one of the above checks fails, the receiver must discard the packet and log the event.
Effect	N/A
Recovery	N/A

75.15 tVrrpRouterAdvNotActivated

Table 1555: tVrrpRouterAdvNotActivated properties

Property name	Value
Application name	VRRP
Event ID	2016
Event name	tVrrpRouterAdvNotActivated
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.11
Default severity	minor
Message format string	Interface *$ifIndex$* of VR *$vrrpOperationsVrId$* is not set to send out Router Advertisement messages using virtual MAC. VR is not allowed to be operational
Cause	The parent interface of the IPv6 VR was not set to send out Router Advertisement and thus the VR was not allowed to become operationally 'up'.
Effect	N/A
Recovery	N/A

75.16 tVrrpRouterAdvNotActivatedClear

Table 1556: tVrrpRouterAdvNotActivatedClear properties

Property name	Value
Application name	VRRP
Event ID	2017
Event name	tVrrpRouterAdvNotActivatedClear
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.12
Default severity	minor
Message format string	tVrrpRouterAdvNotActivated trap from VR *$vrrpOperationsVrId$* on interface *$ifIndex$* has been cleared
Cause	A previously occurring tVrrpRouterAdvNotActivated event has been cleared. The tVrrpRouterAdvNotActivatedClear event is generated when either the parent interface of the IPv6 VR is set to send out Router Advertisement, or the VR is no longer attempting to become active (e.g. the VR is administratively shutdown).
Effect	N/A
Recovery	N/A

75.17 tVrrpTrapNewMaster

Table 1557: tVrrpTrapNewMaster properties

Property name	Value
Application name	VRRP
Event ID	2011
Event name	tVrrpTrapNewMaster
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.7
Default severity	minor
Message format string	VRRP virtual router instance *$vrrpOperationsVrId$* on interface *$if Index$* (primary address *$vrrpOperationsMasterIpAddr$*) changed state to master due to *$vrrpNewMasterReason$*
Cause	The sending agent has transitioned to 'Master' state.
Effect	N/A

Property name	Value
Recovery	N/A

75.18 vrrpPacketDiscarded

Table 1558: vrrpPacketDiscarded properties

Property name	Value
Application name	VRRP
Event ID	2007
Event name	vrrpPacketDiscarded
SNMP notification prefix and OID	N/A
Default severity	minor
Message format string	Discarded VRRP packet from *$vrrpPacketSrc$* because *$vrrpPacket DiscardReason$*
Cause	A VRRP packet was discarded. The following checks are performed on an incoming VRRP packet - verify that the IP TTL is 255. - verify the VRRP version - verify that the received packet length is greater than or equal to the VRRP header - verify the VRRP checksum - perform authentication specified by Auth Type If any one of the above checks fails, the receiver must discard the packet and log the event.
Effect	N/A
Recovery	N/A

75.19 vrrpTrapAuthFailure

Table 1559: vrrpTrapAuthFailure properties

Property name	Value
Application name	VRRP
Event ID	2002
Event name	vrrpTrapAuthFailure
SNMP notification prefix and OID	VRRP-MIB.vrrpNotifications.2
Default severity	minor

Property name	Value
Message format string	Authentication failed for VRRP packet received from *$vrrpTrapPacket Src$* because *$vrrpTrapAuthErrorType$*
Cause	A packet was received from a router whose authentication key or authentication type conflicted with this router's authentication key or authentication type.
Effect	N/A
Recovery	N/A

75.20 vrrpTrapNewMaster

Table 1560: vrrpTrapNewMaster properties

Property name	Value
Application name	VRRP
Event ID	2001
Event name	vrrpTrapNewMaster
SNMP notification prefix and OID	VRRP-MIB.vrrpNotifications.1
Default severity	minor
Message format string	VRRP virtual router instance *$vrrpOperVrId$* on interface *$ifIndex$* (primary address *$vrrpOperMasterIpAddr$*) changed state to master
Cause	Tthe sending agent has transitioned to 'Master' state.
Effect	N/A
Recovery	N/A

75.21 vrrpTrapProtoError

Table 1561: vrrpTrapProtoError properties

Property name	Value
Application name	VRRP
Event ID	2009
Event name	vrrpTrapProtoError

Property name	Value
SNMP notification prefix and OID	VRRP-MIB.vrrpNotifications.3
Default severity	minor
Message format string	VRRP encountered the protocol error due to *$vrrpTrapProtoErrReason $*
Cause	The sending agent encountered a protocol error.
Effect	N/A
Recovery	N/A

76 VRTR

76.1 aluVRtrFibV6TableThresholdExceed

Table 1562: aluVRtrFibV6TableThresholdExceed properties

Property name	Value
Application name	VRTR
Event ID	3001
Event name	aluVRtrFibV6TableThresholdExceed
SNMP notification prefix and OID	ALU-VRTR-MIB.aluVRtrNotifications.2
Default severity	warning
Message format string	TODO
Cause	The aluVRtrFibV6TableThresholdExceed notification is generated when the number of supported V6 routers in FIB on an IOM card transitions between exceeding a high-level water mark and falling below a low-level threshold. Both the high-level water mark and the low-level threshold are defined based on the 7705 platform.
Effect	N/A
Recovery	N/A

76.2 tmnxVRtrArpLmt

Table 1563: tmnxVRtrArpLmt properties

Property name	Value
Application name	VRTR
Event ID	2077
Event name	tmnxVRtrArpLmt
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.77
Default severity	minor

Property name	Value
Message format string	Interface *$vRtrIfName$*: Number of ARP entries learned has exceeded the configured maximum (*$vRtrIfArpLimit$*)
Cause	A tmnxVRtrArpLmt notification is generated when the number of IPv4 ARP entries learned on an IP interface has exceeded the configured maximum.
Effect	The number of entries have exceeded the configured limit as specified by vRtrIfArpLimit. No new entries are learned until an entry expires.
Recovery	Increase the arp-limit.

76.3 tmnxVRtrArpThresholdExceeded

Table 1564: tmnxVRtrArpThresholdExceeded properties

Property name	Value
Application name	VRTR
Event ID	2078
Event name	tmnxVRtrArpThresholdExceeded
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.78
Default severity	minor
Message format string	Interface *$vRtrIfName$*: Number of ARP entries learned has exceeded the *$vRtrIfArpThreshold$* percentage of the configured maximum (*$vRtrIfArpLimit$*)
Cause	A tmnxVRtrArpThresholdExceeded notification is generated when the number of IPv4 ARP entries learned on an IP interface has exceeded vRtrIfArpThreshold percent of the configured maximum as specified by vRtrIfArpLimit.
Effect	No direct effect but if the interface continues to learn more entries then the number of entries may exceed the configured limit as specified by vRtrIfArpLimit. In that case, no new entries are learned until an entry expires and traffic to these destinations will be dropped.
Recovery	Increase the arp-limit.

76.4 tmnxVRtrBfdExtNoCpmNpResources

Table 1565: tmnxVRtrBfdExtNoCpmNpResources properties

Property name	Value
Application name	VRTR
Event ID	2065
Event name	tmnxVRtrBfdExtNoCpmNpResources
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.65
Default severity	minor
Message format string	The BFD session with local discriminator *$vRtrIfBfdSessExtLclDisc$* on node *$subject$* could not be established because cpm-np session termination resources are not available
Cause	The tmnxVRtrBfdExtNoCpmNpResources notification is generated when a BFD session could not be established because the session requires a cpmNp session termination resource (see vRtrIfBfdExtType), and no cpmNp session termination resources are available.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.5 tmnxVRtrBfdMaxSessionOnSlot

Table 1566: tmnxVRtrBfdMaxSessionOnSlot properties

Property name	Value
Application name	VRTR
Event ID	2013
Event name	tmnxVRtrBfdMaxSessionOnSlot
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.18
Default severity	major
Message format string	The number of BFD sessions on *$vRtrSlotOrCpmFlag$ $vRtrBfd SlotNumber$* has exceeded *$vRtrNumberOfBfdSessionsOnSlot$*, constrained by *$vRtrBfdMaxSessionReason$*
Cause	The number of BFD sessions on an IOM or CPM card has exceeded the maximum number allowed.

Property name	Value
Effect	N/A
Recovery	N/A

76.6 tmnxVRtrBfdPortTypeNotSupported

Table 1567: tmnxVRtrBfdPortTypeNotSupported properties

Property name	Value
Application name	VRTR
Event ID	2014
Event name	tmnxVRtrBfdPortTypeNotSupported
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.19
Default severity	major
Message format string	BFD is not supported on *$tmnxPortType$* ports. No sessions will come up on port *$tmnxPortNotifyPortId$*.
Cause	BFD is not supported on the port specified.
Effect	N/A
Recovery	N/A

76.7 tmnxVRtrBfdSessExtDeleted

Table 1568: tmnxVRtrBfdSessExtDeleted properties

Property name	Value
Application name	VRTR
Event ID	2063
Event name	tmnxVRtrBfdSessExtDeleted
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.63
Default severity	minor
Message format string	BFD Session on node *$subject$* has been deleted.

Property name	Value
Cause	The tmnxVRtrBfdSessExtDeleted notification is generated when a BFD session is deleted.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.8 tmnxVRtrBfdSessExtDown

Table 1569: tmnxVRtrBfdSessExtDown properties

Property name	Value
Application name	VRTR
Event ID	2061
Event name	tmnxVRtrBfdSessExtDown
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.61
Default severity	minor
Message format string	BFD: Local Discriminator *$vRtrIfBfdSessExtLclDisc$* BFD session on node *$subject$* is down due to *$vRtrIfBfdSessExtOperFlags$*
Cause	The tmnxVRtrBfdSessExtDown notification is generated when a BFD session goes down.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.9 tmnxVRtrBfdSessExtProtChange

Table 1570: tmnxVRtrBfdSessExtProtChange properties

Property name	Value
Application name	VRTR
Event ID	2064
Event name	tmnxVRtrBfdSessExtProtChange
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.64

Property name	Value
Default severity	minor
Message format string	The protocol(*$vRtrIfBfdSessChangedProtocol$*) using BFD session on node *$subject$* has been *$vRtrIfBfdSessProtoChngdState$*.
Cause	The tmnxVRtrBfdSessExtProtChange notification is generated when there is a change in the list of protocols using the BFD session.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.10 tmnxVRtrBfdSessExtUp

Table 1571: tmnxVRtrBfdSessExtUp properties

Property name	Value
Application name	VRTR
Event ID	2062
Event name	tmnxVRtrBfdSessExtUp
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.62
Default severity	minor
Message format string	BFD: Local Discriminator *$vRtrIfBfdSessExtLclDisc$* BFD session on node *$subject$* is up
Cause	The tmnxVRtrBfdSessExtUp notification is generated when a BFD session goes up.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.11 tmnxVRtrDnsFault

Table 1572: tmnxVRtrDnsFault properties

Property name	Value
Application name	VRTR
Event ID	2066

Property name	Value
Event name	tmnxVRtrDnsFault
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.66
Default severity	minor
Message format string	Fault with DNS server *$vRtrNotifInetAddr$ $vRtrNotifTruthValue$ - $vRtrFailureDescription$*
Cause	The tmnxVRtrDnsFault notification is generated when this system detects a fault with a DNS server, or when it detects that the fault has disappeared. The virtual router instance and DNS server address are indicated with vRtrID, vRtrNotifInetAddrType, and vRtrNotifInetAddr. More details of the fault may be indicated with vRtrFailureDescription.
Effect	If another DNS server is available in the same virtual router instance, that DNS server may be used instead. Otherwise, any application in this virtual router instance that relies on DNS may be affected.
Recovery	A modification of the conceptual row in the vRtrDnsTable with the same value for vRtrID, may repair the problem.

76.12 tmnxVRtrFibOccupancyThreshold

Table 1573: tmnxVRtrFibOccupancyThreshold properties

Property name	Value
Application name	VRTR
Event ID	2023
Event name	tmnxVRtrFibOccupancyThreshold
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.36
Default severity	minor
Message format string	High FIB utilization detected.
Cause	The FIB on an IOM card transitioned between experiencing persistent normal and high utilization.
Effect	N/A
Recovery	N/A

76.13 tmnxVRtrGrtExportLimitReached

Table 1574: tmnxVRtrGrtExportLimitReached properties

Property name	Value
Application name	VRTR
Event ID	2026
Event name	tmnxVRtrGrtExportLimitReached
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.39
Default severity	major
Message format string	GRT has reached the export-limit *$vRtrGrtMaxExportRoutes$*, additional routes will not be exported into GRT
Cause	GRT has exported maximum allowed export routes. It will not export any more routes unless the export policy and export limit is changed.
Effect	GRT will not export any more routes.
Recovery	Change GRT export policy.

76.14 tmnxVRtrGrtRoutesExpLimitDropped

Table 1575: tmnxVRtrGrtRoutesExpLimitDropped properties

Property name	Value
Application name	VRTR
Event ID	2027
Event name	tmnxVRtrGrtRoutesExpLimitDropped
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.40
Default severity	warning
Message format string	The number of exported routes into GRT has dropped below the export limit *$vRtrGrtMaxExportRoutes$*
Cause	Number of exported routes into GRT has dropped below the configured export limit.
Effect	N/A
Recovery	N/A

76.15 tmnxVRtrGrtV6ExportLimitReached

Table 1576: tmnxVRtrGrtV6ExportLimitReached properties

Property name	Value
Application name	VRTR
Event ID	2032
Event name	tmnxVRtrGrtV6ExportLimitReached
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.44
Default severity	major
Message format string	GRT has reached the IPv6 export-limit *$vRtrGrtMaxIpv6ExportRoutes $*, additional routes will not be exported into GRT
Cause	GRT has exported maximum allowed IPv6 export routes. It will not export any more routes unless the export policy and export limit is changed.
Effect	GRT will not export any more routes.
Recovery	Change GRT export policy.

76.16 tmnxVRtrGrtV6RoutesExpLimDropped

Table 1577: tmnxVRtrGrtV6RoutesExpLimDropped properties

Property name	Value
Application name	VRTR
Event ID	2033
Event name	tmnxVRtrGrtV6RoutesExpLimDropped
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.45
Default severity	warning
Message format string	The number of IPv6 exported routes into GRT has dropped below the export limit *$vRtrGrtMaxIpv6ExportRoutes$*
Cause	Number of IPv6 exported routes into GRT has dropped below the configured export limit.
Effect	N/A

Property name	Value
Recovery	N/A

76.17 tmnxVRtrHighRouteCleared

Table 1578: tmnxVRtrHighRouteCleared properties

Property name	Value
Application name	VRTR
Event ID	2003
Event name	tmnxVRtrHighRouteCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.3
Default severity	minor
Message format string	Router *$subject$* has cleared the high-level threshold: *$vRtrHighRoute Threshold$* - the routing table contains *$vRtrStatCurrNumRoutes$* routes
Cause	The number of routes has dropped below the high-level threshold.
Effect	N/A
Recovery	N/A

76.18 tmnxVRtrHighRouteTCA

Table 1579: tmnxVRtrHighRouteTCA properties

Property name	Value
Application name	VRTR
Event ID	2002
Event name	tmnxVRtrHighRouteTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.2
Default severity	minor
Message format string	Router *$subject$* has exceeded the high-level threshold: *$vRtrHigh RouteThreshold$* - the routing table contains *$vRtrStatCurrNumRoutes $* routes

Property name	Value
Cause	The high-level threshold for number of routes has been crossed.
Effect	N/A
Recovery	N/A

76.19 tmnxVRtrIfIgnorePortState

Table 1580: tmnxVRtrIfIgnorePortState properties

Property name	Value
Application name	VRTR
Event ID	2081
Event name	tmnxVRtrIfIgnorePortState
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.81
Default severity	minor
Message format string	Ignoring SAP port state in service: *$vRtrServiceId$* for IP interface: *$vRtrIfName$* is *$vRtrNotifIgnorePortState$*
Cause	The tmnxVRtrIfIgnorePortState notification is generated when ignoring non-operational state of the port associated with the IP interface is changing state.
Effect	This notification is informational only.
Recovery	Set TIMETRA-SAP-MIB::sapL3LoopbackRowStatus to 'destroy' to stop this."

76.20 tmnxVRtrIfLdpSyncTimerStart

Table 1581: tmnxVRtrIfLdpSyncTimerStart properties

Property name	Value
Application name	VRTR
Event ID	2029
Event name	tmnxVRtrIfLdpSyncTimerStart
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.41

Property name	Value
Default severity	warning
Message format string	LDP Sync Timer starts for interface *$vRtrIfName$* with timer value *$vRtrIfLdpSyncTimer$*
Cause	LDP Sync timer started for the interface.
Effect	N/A
Recovery	N/A

76.21 tmnxVRtrIfLdpSyncTimerStop

Table 1582: tmnxVRtrIfLdpSyncTimerStop properties

Property name	Value
Application name	VRTR
Event ID	2030
Event name	tmnxVRtrIfLdpSyncTimerStop
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.42
Default severity	warning
Message format string	LDP Sync Timer stops for interface *$vRtrIfName$* with timer value *$vRtrIfLdpSyncTimer$*
Cause	LDP Sync timer stops for the interface.
Effect	N/A
Recovery	N/A

76.22 tmnxVRtrInetAddressAttachFailed

Table 1583: tmnxVRtrInetAddressAttachFailed properties

Property name	Value
Application name	VRTR
Event ID	2024
Event name	tmnxVRtrInetAddressAttachFailed

Property name	Value
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.37
Default severity	minor
Message format string	Could not attach address *$vRtrNotifInetAddr$* to interface *$vRtrIfIndex$* : *$vRtrFailureDescription$*
Cause	An IP address could not be attached to an interface. A possible cause is that the maximum number of IP addresses in the system is exceeded.
Effect	The IP address cannot be used.
Recovery	N/A

76.23 tmnxVRtrIPv6HighRouteCleared

Table 1584: tmnxVRtrIPv6HighRouteCleared properties

Property name	Value
Application name	VRTR
Event ID	2018
Event name	tmnxVRtrIPv6HighRouteCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.31
Default severity	minor
Message format string	Router *$subject$* has cleared the high-level threshold: *$vRtrIPv6HighRouteThreshold$* - the routing table contains *$vRtrV6StatCurrNumRoutes$* IPv6 routes
Cause	The number of IPv6 routes has dropped below the high-level threshold.
Effect	N/A
Recovery	N/A

76.24 tmnxVRtrIPv6HighRouteTCA

Table 1585: tmnxVRtrIPv6HighRouteTCA properties

Property name	Value
Application name	VRTR
Event ID	2017
Event name	tmnxVRtrIPv6HighRouteTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.30
Default severity	minor
Message format string	Router *$subject$* has exceeded the high-level threshold: *$vRtrIPv6HighRouteThreshold$* - the routing table contains *$vRtrV6StatCurrNumRoutes$* IPv6 routes
Cause	The high-level threshold for number of IPv6 routes has been crossed.
Effect	N/A
Recovery	N/A

76.25 tmnxVRtrIPv6MidRouteTCA

Table 1586: tmnxVRtrIPv6MidRouteTCA properties

Property name	Value
Application name	VRTR
Event ID	2016
Event name	tmnxVRtrIPv6MidRouteTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.29
Default severity	minor
Message format string	Router *$subject$* has exceeded the mid-level threshold: *$vRtrIPv6MidRouteThreshold$* - the routing table contains *$vRtrV6StatCurrNumRoutes$* IPv6 routes
Cause	The mid-level threshold for the number of IPv6 routes has been crossed.
Effect	N/A
Recovery	N/A

76.26 tmnxVRtrIpv6NbrLmt

Table 1587: tmnxVRtrIpv6NbrLmt properties

Property name	Value
Application name	VRTR
Event ID	2079
Event name	tmnxVRtrIpv6NbrLmt
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.79
Default severity	minor
Message format string	Interface *$vRtrIfName$*: Number of neighbor entries learned has exceeded the configured maximum (*$vRtrIfIpv6NbrLimit$*)
Cause	A tmnxVRtrIpv6NbrLmt notification is generated when the maximum amount of IPv6 neighbor entries learned on an IP interface has exceeded the configured maximum.
Effect	The number of entries have exceeded the configured limit as specified by vRtrIfIpv6NbrLimit. No new entries are learned until an entry expires.
Recovery	Increase the neighbor limit.

76.27 tmnxVRtrIpv6NbrThresholdExceeded

Table 1588: tmnxVRtrIpv6NbrThresholdExceeded properties

Property name	Value
Application name	VRTR
Event ID	2080
Event name	tmnxVRtrIpv6NbrThresholdExceeded
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.80
Default severity	minor
Message format string	Interface *$vRtrIfName$*: Number of neighbor entries learned has exceeded the *$vRtrIfIpv6NbrThreshold$* percentage of the configured maximum (*$vRtrIfIpv6NbrLimit$*)

Property name	Value
Cause	A tmnxVRtrIpv6NbrThresholdExceeded notification is generated when the number of IPv6 neighbor entries learned on an IP interface has exceeded vRtrIfIpv6NbrThreshold percent of the configured maximum as specified by vRtrIfIpv6NbrLimit.
Effect	No direct effect but if the interface continues to learn more entries then the number of entries may exceed the configured limit as specified by v RtrIfIpv6NbrLimit. In that case, no new entries are learned until an entry expires and traffic to these destinations will be dropped.
Recovery	Increase the neighbor limit.

76.28 tmnxVRtrMacAcctLimitCleared

Table 1589: tmnxVRtrMacAcctLimitCleared properties

Property name	Value
Application name	VRTR
Event ID	2068
Event name	tmnxVRtrMacAcctLimitCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.68
Default severity	minor
Message format string	Mac Accounting Indices are available for RtrId *$vRtrID$* Interface *$vRtr IfName$*
Cause	The tmnxVRtrMacAcctLimitCleared notification is generated when one or more MAC entries are deleted following the generation of a tmnxVRtrMacAcctLimitReached notification.
Effect	Allocation of further MAC entries will be successful up to the number of entries cleared.
Recovery	No recovery is needed for this notification.

76.29 tmnxVRtrMacAcctLimitReached

Table 1590: tmnxVRtrMacAcctLimitReached properties

Property name	Value
Application name	VRTR
Event ID	2067
Event name	tmnxVRtrMacAcctLimitReached
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.67
Default severity	minor
Message format string	MAC Accounting Limit of 511 has been reached for RtrId *$vRtrID$* Interface *$vRtrIfName$*
Cause	The tmnxVRtrMacAcctLimitReached notification is generated when the system detects that the MAC accounting table is full.
Effect	The MAC accounting table is full and further allocations of accounting indices will fail.
Recovery	The failure can be cleared when the used MAC entries are deleted by disabling MAC accounting on a particular interface or through manual intervention with a user command such as clear router interface mac.

76.30 tmnxVRtrManagedRouteAddFailed

Table 1591: tmnxVRtrManagedRouteAddFailed properties

Property name	Value
Application name	VRTR
Event ID	2022
Event name	tmnxVRtrManagedRouteAddFailed
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.35
Default severity	minor
Message format string	Could not install managed route *$vRtrManagedRouteInetAddr$*/*$vRtrManagedRoutePrefixLen$* in router *$subject$* : *$vRtrFailureDescription$*
Cause	A managed route could not be installed.
Effect	N/A

Property name	Value
Recovery	N/A

76.31 tmnxVRtrMaxArpEntriesCleared

Table 1592: tmnxVRtrMaxArpEntriesCleared properties

Property name	Value
Application name	VRTR
Event ID	2009
Event name	tmnxVRtrMaxArpEntriesCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.9
Default severity	minor
Message format string	Router *$subject$* has cleared the maximum ARP entries threshold: *$vRtrMaxARPEntries$* - its ARP table contains *$vRtrStat ActiveARPEntries$* active entries and *$vRtrStatTotalARPEntries$* total entries
Cause	The number of ARP entries has dropped below the maximum ARP entries threshold for the system.
Effect	N/A
Recovery	N/A

76.32 tmnxVRtrMaxArpEntriesTCA

Table 1593: tmnxVRtrMaxArpEntriesTCA properties

Property name	Value
Application name	VRTR
Event ID	2008
Event name	tmnxVRtrMaxArpEntriesTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.8
Default severity	major

Property name	Value
Message format string	Router *$subject$* has caused the maximum ARP entries threshold for the system to be crossed: *$vRtrMaxARPEntries$* - its ARP table contains *$vRtrStatActiveARPEntries$* active entries and *$vRtrStat TotalARPEntries$* total entries
Cause	The maximum ARP entries threshold for all Routers has been crossed.
Effect	N/A
Recovery	N/A

76.33 tmnxVRtrMaxRoutes

Table 1594: tmnxVRtrMaxRoutes properties

Property name	Value
Application name	VRTR
Event ID	2011
Event name	tmnxVRtrMaxRoutes
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.11
Default severity	minor
Message format string	Router *$subject$* has exceeded the max *$vRtrMaxRoutesType$* routes threshold: *$vRtrMaxNumRoutes$* - the VRF contains *$vRtrStatCurr NumRoutes$* routes
Cause	The maximum routes threshold contained in a VPRN has been crossed.
Effect	N/A
Recovery	N/A

76.34 tmnxVRtrMcastMaxRoutesCleared

Table 1595: tmnxVRtrMcastMaxRoutesCleared properties

Property name	Value
Application name	VRTR
Event ID	2007

Property name	Value
Event name	tmnxVRtrMcastMaxRoutesCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.7
Default severity	minor
Message format string	Router *$subject$* has cleared the high-level threshold for multicast routes: *$vRtrMaxMcastNumRoutes$* - the multicast routing table contains *$vRtrMulticastRoutes$* routes
Cause	The number of multicast routes has dropped below the maximum multicast routes threshold.
Effect	N/A
Recovery	N/A

76.35 tmnxVRtrMcastMaxRoutesTCA

Table 1596: tmnxVRtrMcastMaxRoutesTCA properties

Property name	Value
Application name	VRTR
Event ID	2006
Event name	tmnxVRtrMcastMaxRoutesTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.6
Default severity	minor
Message format string	Router *$subject$* has exceeded the max multicast routes threshold: *$vRtrMaxMcastNumRoutes$* - the multicast routing table contains *$vRtrMulticastRoutes$* routes
Cause	The max routes threshold for number of multicast routes has been crossed.
Effect	N/A
Recovery	N/A

76.36 tmnxVRtrMcastMidRouteTCA

Table 1597: tmnxVRtrMcastMidRouteTCA properties

Property name	Value
Application name	VRTR
Event ID	2005
Event name	tmnxVRtrMcastMidRouteTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.5
Default severity	minor
Message format string	Router *$subject$* has exceeded the mid-level threshold for multicast routes: *$vRtrMcastMidRouteThreshold$* - the multicast routing table contains *$vRtrMulticastRoutes$* routes
Cause	The mid-level threshold for number of multicast routes has been crossed.
Effect	N/A
Recovery	N/A

76.37 tmnxVRtrMidRouteTCA

Table 1598: tmnxVRtrMidRouteTCA properties

Property name	Value
Application name	VRTR
Event ID	2001
Event name	tmnxVRtrMidRouteTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.1
Default severity	minor
Message format string	Router *$subject$* has exceeded the mid-level threshold: *$vRtrMidRoute Threshold$* - the routing table contains *$vRtrStatCurrNumRoutes$* routes
Cause	The mid-level threshold for number of routes has been crossed.
Effect	N/A
Recovery	N/A

76.38 tmnxVRtrNgBfdNoCpmNpResources

Table 1599: tmnxVRtrNgBfdNoCpmNpResources properties

Property name	Value
Application name	VRTR
Event ID	2073
Event name	tmnxVRtrNgBfdNoCpmNpResources
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.73
Default severity	minor
Message format string	The *$vRtrIfBfdSessExtLinkType$* BFD session with local discriminator *$vRtrIfBfdSessExtLclDisc$* on *$subject$* could not be established because cpm-np session termination resources are not available
Cause	The tmnxVRtrNgBfdNoCpmNpResources notification is generated when a BFD session could not be established because the session requires a cpmNp session termination resource (see vRtrIfBfdExtType), and no cpmNp session termination resources are available.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.39 tmnxVRtrNgBfdSessDeleted

Table 1600: tmnxVRtrNgBfdSessDeleted properties

Property name	Value
Application name	VRTR
Event ID	2071
Event name	tmnxVRtrNgBfdSessDeleted
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.71
Default severity	minor
Message format string	*$vRtrIfBfdSessExtLinkType$* BFD session with Local Discriminator *$vRtrIfBfdSessExtLclDisc$* on *$subject$* has been deleted
Cause	The tmnxVRtrNgBfdSessDeleted notification is generated when a BFD session is deleted.

Property name	Value
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.40 tmnxVRtrNgBfdSessDown

Table 1601: tmnxVRtrNgBfdSessDown properties

Property name	Value
Application name	VRTR
Event ID	2069
Event name	tmnxVRtrNgBfdSessDown
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.69
Default severity	minor
Message format string	*$vRtrIfBfdSessExtLinkType$* BFD session with Local Discriminator *$vRtrIfBfdSessExtLclDisc$* on *$subject$* is down due to *$vRtrIfBfdSessExtOperFlags$*
Cause	The tmnxVRtrNgBfdSessDown notification is generated when a BFD session goes down.
Effect	The effect of this session going down is that it either takes down any protocol that is riding over top of it or it notifies them that the session has gone down.
Recovery	The session will automatically attempt to re-establish on it's own.

76.41 tmnxVRtrNgBfdSessProtChange

Table 1602: tmnxVRtrNgBfdSessProtChange properties

Property name	Value
Application name	VRTR
Event ID	2072
Event name	tmnxVRtrNgBfdSessProtChange
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.72

Property name	Value
Default severity	minor
Message format string	The protocol (*$vRtrIfBfdSessChangedProtocol$*) using *$vRtrIfBfdSessExtLinkType$* BFD session on *$subject$* has been *$vRtrIfBfdSessProtoChngdState$*.
Cause	The tmnxVRtrNgBfdSessProtChange notification is generated when there is a change in the list of protocols using the BFD session.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.42 tmnxVRtrNgBfdSessUp

Table 1603: tmnxVRtrNgBfdSessUp properties

Property name	Value
Application name	VRTR
Event ID	2070
Event name	tmnxVRtrNgBfdSessUp
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.70
Default severity	minor
Message format string	*$vRtrIfBfdSessExtLinkType$* BFD session with Local Discriminator *$vRtrIfBfdSessExtLclDisc$* on *$subject$* is up
Cause	The tmnxVRtrNgBfdSessUp notification is generated when a BFD session goes up.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

76.43 tmnxVRtrNHRvplsARPExhaust

Table 1604: tmnxVRtrNHRvplsARPExhaust properties

Property name	Value
Application name	VRTR

Property name	Value
Event ID	2075
Event name	tmnxVRtrNHRvplsARPExhaust
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.75
Default severity	minor
Message format string	The Next Hop RVPLS ARP entries reached 100 percent of its limit *$tmnxVRtrMaxNHRvplsARPEntries$*
Cause	The tmnxVRtrNHRvplsARPExhaust notification is generated when Nexthop RVPLS ARP entries reaches 100% of its limit as indicated by the value of tmnxVRtrMaxNHRvplsARPEntries.
Effect	ARP table reaches high usage limit and further addition of Nexthop RVPLS ARP will fail.
Recovery	Reduce the number of ARPs.

76.44 tmnxVRtrNHRvplsARPHighUsage

Table 1605: tmnxVRtrNHRvplsARPHighUsage properties

Property name	Value
Application name	VRTR
Event ID	2074
Event name	tmnxVRtrNHRvplsARPHighUsage
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.74
Default severity	minor
Message format string	The Next Hop RVPLS ARP entries reached 95 percent of its limit *$tmnxVRtrMaxNHRvplsARPEntries$*
Cause	The tmnxVRtrNHRvplsARPHighUsage notification is generated when Nexthop RVPLS ARP entries reaches 95% of its limit as indicated by the value of tmnxVRtrMaxNHRvplsARPEntries.
Effect	ARP table reaches high usage limit and further addition of Nexthop RVPLS ARP may fail.
Recovery	Reduce the number of ARPs.

76.45 tmnxVRtrNHRvplsARPHighUsageClr

Table 1606: tmnxVRtrNHRvplsARPHighUsageClr properties

Property name	Value
Application name	VRTR
Event ID	2076
Event name	tmnxVRtrNHRvplsARPHighUsageClr
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.76
Default severity	minor
Message format string	The Next Hop RVPLS ARP entries falls below 90 percent of its limit *$tmnxVRtrMaxNHRvplsARPEntries$*
Cause	The tmnxVRtrNHRvplsARPHighUsageClr notification is generated when Nexthop RVPLS ARP entries falls below 90% of its limit following the generation of tmnxVRtrNHRvplsARPHighUsage notification as indicated by the value of tmnxVRtrMaxNHRvplsARPEntries.
Effect	Addition of further Nexthop RVPLS ARP entries will be successful.
Recovery	No recovery is needed for this notification.

76.46 tmnxVRtrSingleSfmOverloadStateCh

Table 1607: tmnxVRtrSingleSfmOverloadStateCh properties

Property name	Value
Application name	VRTR
Event ID	2025
Event name	tmnxVRtrSingleSfmOverloadStateCh
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.38
Default severity	minor
Message format string	The IGP single-SFM overload state changed to : *$vRtrSingleSfm OverloadState$*
Cause	One of the SFM's failed or ISSU is in progress, while single-sfm-overload is enabled on the virtual router instance.
Effect	The system multicast capacity is reduced. The IGP of this virtual router instance enter the overload state, setting the overload bit in IS-IS or

Property name	Value
	setting the metric to maximum in OSPF. PIM will re-route the multicast traffic around this virtual router instance.
Recovery	In case of SFM failure: replace the failed SFM.

76.47 tmnxVRtrStaticRouteCPEStatus

Table 1608: tmnxVRtrStaticRouteCPEStatus properties

Property name	Value
Application name	VRTR
Event ID	2019
Event name	tmnxVRtrStaticRouteCPEStatus
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.32
Default severity	minor
Message format string	On virtual router *$vRtrID$*, the static route CPE check for *$vRtrInetStatRteCpeNotifyAddr$* has transitioned to *$vRtrInetStaticRouteCpeStatus$*.
Cause	A CPE associated with a static route, as specified by the vRtrInetStaticRouteCpeAddr object, became reachable or unreachable.
Effect	N/A
Recovery	N/A

76.48 tmnxVRtrStaticRouteStatusChanged

Table 1609: tmnxVRtrStaticRouteStatusChanged properties

Property name	Value
Application name	VRTR
Event ID	2034
Event name	tmnxVRtrStaticRouteStatusChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.46
Default severity	warning

Property name	Value
Message format string	The current status of the static route of type *$vRtrInetStaticRouteStaticType$* is *$vRtrInetStaticRouteStatus$*. The static route next hop and next hop interface is *$vRtrInetStaticRouteNextHop$* and *$vRtrInetStaticRouteNextHopIf$* respectively.
Cause	The status of a static route has changed from active to inactive or from inactive to active.
Effect	N/A
Recovery	N/A

77 WLAN_GW

77.1 tmnxWlanGwDsmGtpTunnelSetupFail

Table 1610: tmnxWlanGwDsmGtpTunnelSetupFail properties

Property name	Value
Application name	WLAN_GW
Event ID	2012
Event name	tmnxWlanGwDsmGtpTunnelSetupFail
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.16
Default severity	warning
Message format string	The setup of a GTP tunnel for a DSM subscriber failed on MDA *$tmnxCardSlotNum$*/*$tmnxWlanGwNotifyMdaSlotNum$* in WLAN Gateway group *$tmnxWlanGwGrpId$* - *$tmnxWlanGwNotifyDescription$*.
Cause	A problem occurred while trying to setup a GTP tunnel for a DSM subscriber. This can be caused by: - incomplete system configuration, or - inconsistent RADIUS configuration, or - because the GTP peer is not reachable.
Effect	The DSM subscriber cannot establish a connection with his home mobile network.
Recovery	Depending on the cause, correct the system configuration, the RADIUS configuration or the network connectivity.

77.2 tmnxWlanGwGrpOperStateChanged

Table 1611: tmnxWlanGwGrpOperStateChanged properties

Property name	Value
Application name	WLAN_GW
Event ID	2004
Event name	tmnxWlanGwGrpOperStateChanged
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.4

Property name	Value
Default severity	minor
Message format string	The state of WLAN Gateway group *$tmnxWlanGwGrpId$* changed to *$tmnxWlanGwGrpOperState$*.
Cause	The tmnxWlanGwGrpOperStateChanged notification is sent when the value of the object tmnxWlanGwGrpOperState changes.
Effect	N/A
Recovery	N/A

77.3 tmnxWlanGwGtpMessageDropped

Table 1612: tmnxWlanGwGtpMessageDropped properties

Property name	Value
Application name	WLAN_GW
Event ID	2020
Event name	tmnxWlanGwGtpMessageDropped
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.24
Default severity	warning
Message format string	GTP *$tmnxWlanGwNotifyGtpMsgDirection$* message (type *$tmnx WlanGwNotifyGtpMsgType$* version *$tmnxWlanGwMgwControl$* IMSI *$tmnxWlanGwNotifyImsi$* TEID *$tmnxWlanGwNotifyTeid$*) dropped from/to Mobile Gateway *$tmnxWlanGwMgwRemoteAddr$* port *$tmnx WlanGwMgwRemotePort$* in router *$vRtrID$* - *$tmnxWlanGwNotify Description$*
Cause	The cause is indicated in the tmnxWlanGwNotifyDescription.
Effect	The effect depends on the dropped message and the state of the system.
Recovery	The recovery, if any, depends on the reason the message was dropped.

77.4 tmnxWlanGwIomActive

Table 1613: tmnxWlanGwIomActive properties

Property name	Value
Application name	WLAN_GW
Event ID	2005
Event name	tmnxWlanGwIomActive
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.5
Default severity	minor
Message format string	The WLAN Gateway IOM *$tmnxCardSlotNum$* of group *$tmnxWlanGwGrpId$* is now *$tmnxWlanGwTrue$*.
Cause	The tmnxWlanGwIomActive notification is sent when the value of the object tmnxWlanGwIomOperState changes from 'primary' to any other value, or the other way around. The value 'primary' means that the IOM is active in the group.
Effect	N/A
Recovery	N/A

77.5 tmnxWlanGwMgwConnected

Table 1614: tmnxWlanGwMgwConnected properties

Property name	Value
Application name	WLAN_GW
Event ID	2006
Event name	tmnxWlanGwMgwConnected
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.10
Default severity	minor
Message format string	The connection with Mobile Gateway is established.
Cause	A connection is established between this system's WLAN Gateway function and a Mobile Gateway, or such a connection disappears. The interruption of a connection with a Mobile Gateway can be the expected result of a management action on the Mobile Gateway, or it can be caused by a network failure.

Property name	Value
Effect	While there is a connection with a particular Mobile Gateway, User Equipment (UE) belonging to the associated PLMN (Public Land Mobile Network) and serviced by this WLAN Gateway can be connected to their Home PLMN.
Recovery	If a connection with a Mobile Gateway is interrupted as the expected result of a management action, no recovery is required.

77.6 tmnxWlanGwMgwRestarted

Table 1615: tmnxWlanGwMgwRestarted properties

Property name	Value
Application name	WLAN_GW
Event ID	2007
Event name	tmnxWlanGwMgwRestarted
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.11
Default severity	minor
Message format string	The Mobile Gateway has restarted. The restart count is *$tmnxWlan GwMgwRestartCount$*.
Cause	A Mobile Gateway known to this system has restarted, has transmitted its restart counter to this system and it was found to be higher than its previously known value.
Effect	This system clears all sessions associated with the restarted Mobile Gateway (because that Mobile Gateway has lost its session data anyway).
Recovery	No recovery is required on this system.

77.7 tmnxWlanGwMgwStateChanged

Table 1616: tmnxWlanGwMgwStateChanged properties

Property name	Value
Application name	WLAN_GW
Event ID	2009

Property name	Value
Event name	tmnxWlanGwMgwStateChanged
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.13
Default severity	minor
Message format string	The state of the Mobile Gateway has changed to *$tmnxWlanGwMgwState$*.
Cause	The state of a connection with a Mobile Gateway has changed.
Effect	The effect depends on the new state.
Recovery	No recovery is required on this system.

77.8 tmnxWlanGwNumMgwHi

Table 1617: tmnxWlanGwNumMgwHi properties

Property name	Value
Application name	WLAN_GW
Event ID	2008
Event name	tmnxWlanGwNumMgwHi
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.12
Default severity	minor
Message format string	The number of Mobile Gateways connected to this system (*$tmnxWlanGwNumGw$*) is high (*$tmnxWlanGwNotifyTrue$*).
Cause	The number of Mobile Gateways connected to this system is approaching the maximum supported value.
Effect	If the increasing trend continues, this system will not be able to connect some User Equipment (UE) with their Home PLMN.
Recovery	The network configuration may have to be modified such that this system will be associated with less Mobile Gateways.

77.9 tmnxWlanGwQosRadiusGtpMismatch

Table 1618: tmnxWlanGwQosRadiusGtpMismatch properties

Property name	Value
Application name	WLAN_GW
Event ID	2010
Event name	tmnxWlanGwQosRadiusGtpMismatch
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.14
Default severity	minor
Message format string	There is a mismatch between the 3GPP release *$tmnxWlan GwNotify3gppRelease$* in the RADIUS Negotiated QoS profile, and the interface type *$tmnxWlanGwMgwInterfaceType$* of the Mobile Gateway.
Cause	Inconsistency between the release indicator in the RADIUS attribute and the GTP interface type.
Effect	The QoS values in the tmnxWlanGwPgwTable or the tmnxWlan GwGgsnTable of the conceptual row corresponding to the row in the tmnxWlanGwMgwAddrTable that matches the WLAN are used instead.
Recovery	The RADIUS Server configuration should be corrected.

77.10 tmnxWlanGwResrcProblemCause

Table 1619: tmnxWlanGwResrcProblemCause properties

Property name	Value
Application name	WLAN_GW
Event ID	2002
Event name	tmnxWlanGwResrcProblemCause
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.2
Default severity	minor
Message format string	*$tmnxWlanGwNotifyDescription$*.
Cause	The tmnxWlanGwResrcProblemCause notification is sent to describe the cause of a WLAN Gateway resource problem.
Effect	N/A

Property name	Value
Recovery	N/A

77.11 tmnxWlanGwResrcProblemDetected

Table 1620: tmnxWlanGwResrcProblemDetected properties

Property name	Value
Application name	WLAN_GW
Event ID	2001
Event name	tmnxWlanGwResrcProblemDetected
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.1
Default severity	minor
Message format string	The status of the WLAN GW resource problem indication changed to *$tmnxWlanGwResrcProblem$*.
Cause	The tmnxWlanGwResrcProblemDetected notification is sent when the value of the object tmnxWlanGwResrcProblem changes.
Effect	N/A
Recovery	N/A

77.12 tmnxWlanGwSubIfPmAddNewPlFailed

Table 1621: tmnxWlanGwSubIfPmAddNewPlFailed properties

Property name	Value
Application name	WLAN_GW
Event ID	2015
Event name	tmnxWlanGwSubIfPmAddNewPlFailed
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.19
Default severity	minor
Message format string	Failed to add a new pool given by the DHCPv6 server. (service *$svc Id$*, interface *$tmnxWlanGwNotifySubIfIndex$*, address-family *$tmnx WlanGwNotifyAddrFamily$*)

Property name	Value
Cause	Failed to add a new pool given by the server.
Effect	The ISA-BB may run out of free DHCPv6 addresses or SLAAC prefixes.
Recovery	No recovery is needed. Retry periodically.

77.13 tmnxWlanGwSubIfPmCrIntObjFailed

Table 1622: tmnxWlanGwSubIfPmCrIntObjFailed properties

Property name	Value
Application name	WLAN_GW
Event ID	2016
Event name	tmnxWlanGwSubIfPmCrIntObjFailed
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.20
Default severity	minor
Message format string	Failed to create an internal object for a pool. (service *$svcId$*, interface *$tmnxWlanGwSubIfIpsSubIfIndex$*, address *$tmnxWlanGwSubIfIps SubnetAddr$*, prefix-length *$tmnxWlanGwSubIfIpsSubnetPrefLen$*, address-family *$tmnxWlanGwNotifyAddrFamily$*, description *$tmnx WlanGwNotifyDescription$*)
Cause	Failed to create an internal object for a pool.
Effect	Forwarding will not work for UEs having an address/prefix from this pool.
Recovery	No recovery is needed. Retry periodically.

77.14 tmnxWlanGwSubIfPmLsQryRtryFailed

Table 1623: tmnxWlanGwSubIfPmLsQryRtryFailed properties

Property name	Value
Application name	WLAN_GW
Event ID	2019
Event name	tmnxWlanGwSubIfPmLsQryRtryFailed

Property name	Value
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.23
Default severity	minor
Message format string	The lease query retry failed.
Cause	Lease query retry failed.
Effect	The old prefix couldn't be fetched from the DHCP server.
Recovery	No recovery possible.

77.15 tmnxWlanGwSubIfPmNewPlReqFailed

Table 1624: tmnxWlanGwSubIfPmNewPlReqFailed properties

Property name	Value
Application name	WLAN_GW
Event ID	2014
Event name	tmnxWlanGwSubIfPmNewPlReqFailed
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.18
Default severity	minor
Message format string	Failed to send a request for a new pool. (service *$svcId$*, interface *$tmnxWlanGwNotifySubIfIndex$*, address-family *$tmnxWlanGwNotify AddrFamily$*)
Cause	Failed to send a request for a new pool.
Effect	The ISA-BB may run out of free DHCPv6 addresses or SLAAC prefixes.
Recovery	No recovery is needed. Retry periodically.

77.16 tmnxWlanGwSubIfPmPoolTimeout

Table 1625: tmnxWlanGwSubIfPmPoolTimeout properties

Property name	Value
Application name	WLAN_GW

Property name	Value
Event ID	2017
Event name	tmnxWlanGwSubIfPmPoolTimeout
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.21
Default severity	minor
Message format string	The pool timed out unexpectedly. (address-family *$tmnxWlanGwNotifyAddrFamily$*, description *$tmnxWlanGwNotifyDescription$*)
Cause	Pool timed out unexpectedly.
Effect	The pool is removed from the ISA-BB together with all associated UEs.
Recovery	No recovery possible.

77.17 tmnxWlanGwSubIfPmPoolUsageLow

Table 1626: tmnxWlanGwSubIfPmPoolUsageLow properties

Property name	Value
Application name	WLAN_GW
Event ID	2018
Event name	tmnxWlanGwSubIfPmPoolUsageLow
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.22
Default severity	minor
Message format string	The usage of a pool dropped below 1%. (address-family *$tmnxWlanGwNotifyAddrFamily$*)
Cause	Pool usage dropped below 1%.
Effect	The pool has become stale.
Recovery	Manually clear the pool.

77.18 tmnxWlanGwSubIfPmStartD6cFailed

Table 1627: tmnxWlanGwSubIfPmStartD6cFailed properties

Property name	Value
Application name	WLAN_GW
Event ID	2013
Event name	tmnxWlanGwSubIfPmStartD6cFailed
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.17
Default severity	minor
Message format string	The DHCPv6 client of the Pool Manager failed to start. (service *$svc Id$*, interface *$tmnxWlanGwNotifySubIfIndex$*, address-family *$tmnx WlanGwNotifyAddrFamily$*)
Cause	Failed to start a DHCPv6 client.
Effect	No pools can be requested for this ISA-BB.
Recovery	Perform a shutdown/no shutdown of the DHCPv6 client.

77.19 tmnxWlanGwSubIfRedActiveChanged

Table 1628: tmnxWlanGwSubIfRedActiveChanged properties

Property name	Value
Application name	WLAN_GW
Event ID	2011
Event name	tmnxWlanGwSubIfRedActiveChanged
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.15
Default severity	warning
Message format string	The WLAN Gateway function on interface $$ is now *$tmnxWlanGwSub IfRedActive$ - $tmnxWlanGwNotifyDescription$*
Cause	To be documented
Effect	To be documented
Recovery	No recovery is required on this system.

77.20 tmnxWlanGwTuQosProblem

Table 1629: tmnxWlanGwTuQosProblem properties

Property name	Value
Application name	WLAN_GW
Event ID	2003
Event name	tmnxWlanGwTuQosProblem
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.3
Default severity	minor
Message format string	The value of tmnxWlanGwIsaMemberTuQosProblem has changed to *$tmnxWlanGwIsaMemberTuQosProblem$*.
Cause	While creating a WLAN Gateway tunnel QoS infrastructure instance, there was a resource issue.
Effect	There are UE with a QoS infrastructure that does not match the configuration, for example: no shaper was instantiated.
Recovery	This may be a temporary phenomenon. If it persists, the QoS configuration or the scaling may have to be modified to ensure enough resources are available for the UE QoS.

78 WPP

78.1 tmnxWppHostAuthenticationFailed

Table 1630: tmnxWppHostAuthenticationFailed properties

Property name	Value
Application name	WPP
Event ID	2002
Event name	tmnxWppHostAuthenticationFailed
SNMP notification prefix and OID	TIMETRA-WEB-PORTAL-PROTOCOL-MIB.tmnxWppNotifications.2
Default severity	warning
Message format string	WPP host (router *$vRtrID$*, portal *$tmnxWppPortalName$*, address *$tmnxWppHostAddr$*) could not be authenticated - *$tmnxWppNotify Description$*.
Cause	The tmnxWppHostAuthenticationFailed notification is sent when a WPP host could not be authenticated. Mored detailed information is supplied in the object tmnxWppNotifyDescription.
Effect	The corresponding row in the tmnxWppHostTable disappears if the value of the object tmnxWppIfRestoreDisconnected is equal to 'false'; otherwise, the value of the object tmnxWppHostStatus is set to 'idle'.
Recovery	The recovery action will depend on the exact failure cause, as given by the value of tmnxWppNotifyDescription.

78.2 tmnxWppPortalStatChanged

Table 1631: tmnxWppPortalStatChanged properties

Property name	Value
Application name	WPP
Event ID	2001
Event name	tmnxWppPortalStatChanged
SNMP notification prefix and OID	TIMETRA-WEB-PORTAL-PROTOCOL-MIB.tmnxWppNotifications.1

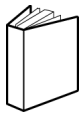
Property name	Value
Default severity	warning
Message format string	The state of portal *$tmnxWppPortalName$* in router *$vRtrID$* has changed to (controlled router = *$tmnxWppPortalStateControlledRtr$*, number of interfaces = *$tmnxWppPortalStateNumInterfaces$*).
Cause	The tmnxWppPortalStatChanged notification is sent when the value of one of the objects in the tmnxWppPortalStatTable changes.
Effect	No effect on the service.
Recovery	No recovery required.

78.3 tmnxWppPortalUnreachable

Table 1632: tmnxWppPortalUnreachable properties

Property name	Value
Application name	WPP
Event ID	2003
Event name	tmnxWppPortalUnreachable
SNMP notification prefix and OID	TIMETRA-WEB-PORTAL-PROTOCOL-MIB.tmnxWppNotifications.3
Default severity	minor
Message format string	WPP portal (router *$vRtrID$*, portal *$tmnxWppPortalName$*) is unreachable - *$tmnxWppNotifyDescription$*.
Cause	The tmnxWppPortalUnreachable notification is generated when WPP protocol messages must be sent out after a node is restarted, but when no route is available yet towards it. This notification is sent every minute as long as the portal is not reachable yet.
Effect	The WPP portal is unreachable and finally the messages will be dropped.
Recovery	Initially no recovery is required as it is expected that the WPP portal can be unreachable for some time after a node restart. When however the problem remains the operator should check the routing table.

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback