7250 Interconnect Router
7450 Ethernet Service Switch
7750 Service Router
7950 Extensible Routing System
Virtualized Service Router

Release 24.10.R1

Log Events Guide

3HE 20099 AAAC TQZZA 01
Edition: 01
October 2024

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 overview

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

For more information about event logs, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide* or the *7250 IXR System Management Guide*.

1.1 About log events

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

- A time stamp in UTC or local time.
- The generating application.
- A unique event ID within the application.
- A router name identifying the router instance that generated the event.
- A subject identifying the affected object.
- A short text description.

Note: The Message Format String lists the log event parameters available when the log event is output in CLI using the **show log** command, output to a file for file-based event logs, or output to a syslog receiver. However, for some log events their parameters may vary when the event is output to SNMP destination, NETCONF destination, or triggers an EHS script. To see a complete list of a log event parameters available to EHS scripts and NETCONF notifications, use the CLI command **show log event-parameters** for that specific event. For further information about variables found in the message format strings, please see the associated SNMP Notification definition in the SR OS MIBs.

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

```
nnnn <time> TZONE <severity>: <application> #<event-id> <vrtr-name> <subject>
<message>
```

Example

```
252 2013/05/07 16:21:00.76 UTC WARNING: SNMP #2005 Base my-interface-abc
"Interface my-interface-abc is operational"
```

The specific elements that compose the general format are described in Table 1: Log Entry Field Descriptions.

Table 1: Log Entry Field Descriptions

Label	Description
nnnn	The log entry sequence number.
<time>	The UTC or local date stamp for the log entry in YYYY/MM/DD format followed by the UTC time stamp in HH:MM:SS.SS format. *YYYY* — Year *MM* — Month *DD* — Date *HH* — Hour *MM* — Minute *SS.SS* — Seconds
TZONE	The time zone (for example, UTC, EDT) as configured by **configure log log-id** *x* **time-format**.
<severity>	The severity level of the event: • critical — A critical severity event • major — A major severity event • minor — A minor severity event • warning — A warning severity event • cleared — A cleared event • indeterminate — An indeterminate/informational severity event **Note:** The term "INFO" may appear in messages in management interfaces indicating a situation that is less impactful than a "warning", or a situation that has an indeterminate impact, but "INFO" is not a log event severity in SR OS.
<application>	The name of the application generating the log message.
<event-id>	The application event ID number.
<vrtr-name>	The router name (vrtr-name, for example, vprn101 or Base), in a format used by the logging system, representing the router instance that generated the event.
<subject>	The subject/affected object for the event.
<message>	A text description of the event for CLI (**show log**), log files and syslog output.

Label	Description
	The variables in the <message> string do not necessarily apply to SNMP, NETCONF or EHS scripts. For the list of variables available to EHS scripts and NETCONF notifications, use the CLI command **show log event-parameters**. For further information about variables found in the <message> strings, please see the associated SNMP Notification definition in the SR OS MIBs.

1.2 Sample log event

Table 2: cli_config_io properties contains a sample log event entry from this guide for the cli_config_io log event.

Table 2: 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
Source stream	change
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	The user entered an authorized configuration command in the classic CLI.
Effect	The configuration was changed by the 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 Table 3: Log Entry Field Descriptions .

Table 3: Log Entry Field Descriptions

Label	Description
Application name	The name of the application generating the log message.
Event id	The application event ID number.

Label	Description
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, or "N/A" for event types that do not generate an associated SNMP notification.
Default severity	The default severity level of the event. • critical • major • minor • warning • cleared
Source stream	The event source. • main • security • change • debug • li
Message format string	A text description of the event for CLI (**show log**), log files and syslog output. The variables in the 'Message format string' do not necessarily apply to SNMP, NETCONF or EHS scripts. For the list of variables available to EHS scripts and NETCONF notifications, use the CLI command **show log event-parameters**. For further information about variables found in the 'Message format string', please see the associated SNMP Notification definition in the SR OS MIBs.
Cause	The cause of the event.
Effect	The effect of the event.
Recovery	How to recover from this event, if necessary.

2 ADP

2.1 tmnxDiscoveryCellularReq

Table 4: tmnxDiscoveryCellularReq properties

Property name	Value
Application name	ADP
Event ID	2050
Event name	tmnxDiscoveryCellularReq
SNMP notification prefix and OID	TIMETRA-DISCOVERY-MIB.tmnxDiscoveryNotifications.1
Default severity	minor
Source stream	main
Message format string	NMS Cellular PDN Configuration Request sent
Cause	N/A
Effect	N/A
Recovery	N/A

2.2 tmnxDiscoveryEndNotify

Table 5: tmnxDiscoveryEndNotify properties

Property name	Value
Application name	ADP
Event ID	2005
Event name	tmnxDiscoveryEndNotify
SNMP notification prefix and OID	TIMETRA-DISCOVERY-MIB.tmnxDiscoveryNotifications.2

Property name	Value
Default severity	minor
Source stream	main
Message format string	Auto-Discovery process has ended
Cause	N/A
Effect	N/A
Recovery	N/A

3 ANYSEC

3.1 tmnxAnySecMkaOperStateChanged

Table 6: tmnxAnySecMkaOperStateChanged properties

Property name	Value
Application name	ANYSEC
Event ID	2002
Event name	tmnxAnySecMkaOperStateChanged
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.2
Default severity	warning
Source stream	main
Message format string	MKA Oper State Changed to *$tmnxAnySecMkaStatsOperStateNotif$* - Encryption Group: *$tmnxAnySecEncryptGroupNameNotif$*, Remote Peer: *$tmnxAnySecPeerAddrNotif$*, CAK Name: *$tmnxAnySecCak NameNotif$*
Cause	The tmnxAnySecMkaOperStateChanged notification is sent when a change occurs in the operational state of the MACSec Key Agreement (MKA) used by the Connectivity Association (CA) specified for the specified encryption group.
Effect	Informational.
Recovery	N/A.

3.2 tmnxAnySecMkaPskRollover

Table 7: tmnxAnySecMkaPskRollover properties

Property name	Value
Application name	ANYSEC

Property name	Value
Event ID	2001
Event name	tmnxAnySecMkaPskRollover
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.1
Default severity	warning
Source stream	main
Message format string	PSK Rollover for MKA over IP - Encryption Group: *$tmnxAnySec EncryptGroupNameNotif$*, Remote Peer: *$tmnxAnySecPeerAddrNotif $*, CAK Name: *$tmnxAnySecNewCakNameNotif$*, Key Entry Number: *$tmnxAnySecKeyEntryNumberNotif$*
Cause	The tmnxAnySecMkaPskRollover notification is sent when a pre-shared key (PSK) rollover occurs for the MACSec Key Agreement (MKA) used by the Connectivity Association (CA) specified for the specified encryption group.
Effect	Informational.
Recovery	N/A.

3.3 tmnxAnySecMkaSessionEnded

Table 8: tmnxAnySecMkaSessionEnded properties

Property name	Value
Application name	ANYSEC
Event ID	2010
Event name	tmnxAnySecMkaSessionEnded
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.10
Default severity	warning
Source stream	main
Message format string	ANYsec MKA session ended with for peer *$tmnxAnySecPeerAddr$* in encryption group *$tmnxAnySecEncryptGrpName$* with MI:SCI *$tmnx AnySecMkaStatsMemberId$*: *$tmnxAnySecMkaStatsOutboundSci$* CA *$tmnxAnySecEncryptGrpCAName$* peer MI *$tmnxAnySecPeer MemberIdNotif$*

Property name	Value
Cause	A tmnxAnySecMkaSessionEnded notification is generated when an MKA session is ended.
Effect	N/A
Recovery	N/A

3.4 tmnxAnySecMkaSessionEstablished

Table 9: tmnxAnySecMkaSessionEstablished properties

Property name	Value
Application name	ANYSEC
Event ID	2009
Event name	tmnxAnySecMkaSessionEstablished
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.9
Default severity	warning
Source stream	main
Message format string	ANYsec MKA session established for peer *$tmnxAnySecPeerAddr$* in encryption group *$tmnxAnySecEncryptGrpName$* with MI:SCI *$tmnxAnySecMkaStatsMemberId$*:*$tmnxAnySecMkaStatsOutboundSci$* CA *$tmnxAnySecEncryptGrpCAName$* local key-server priority *$tmnxAnySecMkaLocalKSPrioNotif$* peer key-server priority *$tmnxAnySecMkaPeerKSPrioNotif$* cipher-suite *$tmnxAnySecMkaStatsOperCipher$* peer MI *$tmnxAnySecPeerMemberIdNotif$*
Cause	A tmnxAnySecMkaSessionEstablished notification is generated when an MKA session is established.
Effect	N/A
Recovery	N/A

3.5 tmnxAnySecMkaSessionInitiation

Table 10: tmnxAnySecMkaSessionInitiation properties

Property name	Value
Application name	ANYSEC
Event ID	2003
Event name	tmnxAnySecMkaSessionInitiation
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.3
Default severity	warning
Source stream	main
Message format string	ANYsec MKA session initiated for peer *$tmnxAnySecPeerAddrNotif$* in encryption group *$tmnxAnySecEncryptGroupNameNotif$*
Cause	The tmnxAnySecMkaSessionInitiation notification is sent when all of the four entities (security termination policy, connectivity association, encryption group, and peer) associated with an ANYsec MKA session are administratively enabled.
Effect	The enabling of all associated entities causes the initiation of the ANYsec MKA session and MKA session negotiation will begin. If negotiation is successful, notification tmnxAnySecMkaOperState Changed will be sent with a change to 'up'.
Recovery	N/A.

3.6 tmnxAnySecMkaSessionTermination

Table 11: tmnxAnySecMkaSessionTermination properties

Property name	Value
Application name	ANYSEC
Event ID	2004
Event name	tmnxAnySecMkaSessionTermination
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.4
Default severity	warning
Source stream	main

Property name	Value
Message format string	ANYsec MKA session terminated for peer *$tmnxAnySecPeerAddrNotif $* in encryption group *$tmnxAnySecEncryptGroupNameNotif$ - $tmnx AnySecMkaSessTermReasonNotif$* is administratively disabled - traffic is being dropped
Cause	The tmnxAnySecMkaSessionTermination notification is sent when either the security termination policy or the connectivity association associated with the ANYsec MKA session is administratively disabled. This notification is not sent when either the associated peer or encryption group is administratively disabled because the disabling of either of those causes unencrypted traffic to be transmitted resulting in the critical notification tmnxAnySecSessionDisabled being sent.
Effect	The disabling of either the security termination policy or the connectivity association causes the termination of the ANYsec MKA session. The associated MKA encryption will stop, and its traffic will be dropped in the data path.
Recovery	To restart transmission, enable all entities associated with the MKA session.

3.7 tmnxAnySecPeerInconsisRxSciClrd

Table 12: tmnxAnySecPeerInconsisRxSciClrd properties

Property name	Value
Application name	ANYSEC
Event ID	2008
Event name	tmnxAnySecPeerInconsisRxSciClrd
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.8
Default severity	warning
Source stream	main
Message format string	ANYsec inconsistent Rx SCI cleared - transmission to peer *$tmnxAny SecPeerAddrNotif$* in encryption group *$tmnxAnySecEncryptGroup NameNotif$* resumed
Cause	The tmnxAnySecPeerInconsisRxSciClrd notification is sent when the condition that caused the previous tmnxAnySecPeerInconsisRxSci Dtctd to be triggered is cleared, i.e.: the peer encryption SID label is made to be consistent with the local encryption SID label.

Property name	Value
Effect	Traffic will be sent to this peer.
Recovery	N/A, informational.

3.8 tmnxAnySecPeerInconsisRxSciDtctd

Table 13: tmnxAnySecPeerInconsisRxSciDtctd properties

Property name	Value
Application name	ANYSEC
Event ID	2007
Event name	tmnxAnySecPeerInconsisRxSciDtctd
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.7
Default severity	warning
Source stream	main
Message format string	ANYsec inconsistent Rx SCI detected - transmission to peer *$tmnxAnySecPeerAddrNotif$* in encryption group *$tmnxAnySecEncryptGroupNameNotif$* stopped - Rx SCI: *$tmnxAnySecPeerIncsRxSciNotif$* - reason: *$tmnxAnySecPeerIncsRxSciResnNotif$*
Cause	The tmnxAnySecPeerInconsisRxSciDtctd notification is sent when the peer sends an SCI that is not consistent with the local encryption SID label.
Effect	Traffic will not be sent to this peer.
Recovery	To resume transmission, the peer encryption SID label must be made consistent with the local encryption SID label.

3.9 tmnxAnySecSessionDisabled

Table 14: tmnxAnySecSessionDisabled properties

Property name	Value
Application name	ANYSEC

Property name	Value
Event ID	2006
Event name	tmnxAnySecSessionDisabled
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.6
Default severity	critical
Source stream	main
Message format string	ANYsec session disabled for peer *$tmnxAnySecPeerAddrNotif$* (peer admin state: *$tmnxAnySecPeerAdminState$*) in encryption group *$tmnxAnySecEncryptGroupNameNotif$* (group admin state: *$tmnxAnySecEncryptGrpAdminState$*) - Clear text transmission occurring
Cause	The tmnxAnySecSessionEnabled notification is sent when either a peer or its associated encryption group is administratively disabled.
Effect	Encryption of traffic to the peer will be stopped and clear text traffic will be transmitted.
Recovery	To resume encryption (and stop clear text transmission), administratively enable both the peer and its associated encryption group.

3.10 tmnxAnySecSessionEnabled

Table 15: tmnxAnySecSessionEnabled properties

Property name	Value
Application name	ANYSEC
Event ID	2005
Event name	tmnxAnySecSessionEnabled
SNMP notification prefix and OID	TIMETRA-ANYSEC-MIB.tmnxAnySecNotifications.5
Default severity	warning
Source stream	main
Message format string	ANYsec session enabled for peer *$tmnxAnySecPeerAddrNotif$* in encryption group *$tmnxAnySecEncryptGroupNameNotif$*
Cause	The tmnxAnySecSessionEnabled notification is sent when a peer and its associated encryption group are both administratively enabled.

Property name	Value
Effect	Encrypted traffic will be transmitted to the specified peer when tmnxAnySecMkaStatsOperState transitions to 'up'. Until tmnxAnySecMkaStatsOperState transitions to 'up', traffic will be dropped.
Recovery	N/A.

4 APPLICATION_ASSURANCE

4.1 tmnxBsxAarpInstOperStateChanged

Table 16: 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
Source stream	main
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.

4.2 tmnxBsxAarpInstStateChanged

Table 17: tmnxBsxAarpInstStateChanged properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4436

Property name	Value
Event name	tmnxBsxAarpInstStateChanged
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.36
Default severity	warning
Source stream	main
Message format string	Status of AARP instance *$tmnxBsxAarpInstId$* changed state: *$tmnxBsxAarpInstState$*, flags = *$tmnxBsxAarpInstOperFlags$*
Cause	A tmnxBsxAarpInstStateChanged notification is generated when the state of the AARP instance changes.
Effect	None.
Recovery	No recovery is required.

4.3 tmnxBsxAaSubPolResExceeded

Table 18: 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
Source stream	main
Message format string	Policer resources have been exceeded for subscribers in group *$tmnxBsxNotifyAaGrpPartIndex$*.
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.

4.4 tmnxBsxAaSubPolResExceededClear

Table 19: tmnxBsxAaSubPolResExceededClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4414
Event name	tmnxBsxAaSubPolResExceededClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.14
Default severity	warning
Source stream	main
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.

4.5 tmnxBsxAaSubscriberAcctDataLoss

Table 20: 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
Source stream	main

Property name	Value
Message format string	Accounting data loss occurred for subscriber *$tmnxBsxNotifyAaSubscriberName$*.
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.

4.6 tmnxBsxAaSubscribersUnassigned

Table 21: 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
Source stream	main
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.

4.7 tmnxBsxCertProfileOperStateChngd

Table 22: tmnxBsxCertProfileOperStateChngd properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4462
Event name	tmnxBsxCertProfileOperStateChngd
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.62
Default severity	minor
Source stream	main
Message format string	The operational state of certificate profile *$tmnxBsxNotifyCertProfile Name$* in ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* is *$tmnx BsxNotifyCertProfOperState$*. Reason: *$tmnxBsxNotifyReason$*
Cause	A tmnxBsxCertProfileOperStateChngd notification is generated when the operational state of the certificate-profile is changed. The tmnxBsx NotifyReason will identify the reason. Most common cause are: - use of an unsupported algorithm. - use of a key with unsupported key length. - file permissions
Effect	Functions dependent on the certificate profiles may not work as expected, if the operational state is outOfService(3).
Recovery	Resolve the condition as reported in tmnxBsxNotifyReason.

4.8 tmnxBsxDatapathCpuUsage

Table 23: 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

Property name	Value
Default severity	minor
Source stream	main
Message format string	Datapath CPU usage is greater than or equal to *$tmnxBsxDatapathCpuHighWatermark$*% on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* in group *$tmnxBsxNotifyIsaAaGroupIndex$*.
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 tmnxBsxIsaAaGrpOverloadCutThru is 'enabled (1)' for the Application Assurance group.
Recovery	There is no recovery for this notification.

4.9 tmnxBsxDatapathCpuUsageClear

Table 24: 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
Source stream	main
Message format string	Datapath CPU usage is less than or equal to *$tmnxBsxDatapathCpuLowWatermark$*% on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* 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.

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

4.10 tmnxBsxDnsIpCacheFull

Table 25: 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
Source stream	main
Message format string	The usage of ISA-AA Group *$tmnxBsxIsaAaGroupIndex$* DNS IP Cache " *$tmnxBsxDnsIpCacheName$*" for ISA-MDA *$tmnxBsxNotifyIsaMdaNum$* is greater than or equal to the *$tmnxBsxDnsIpCacheHighWatermark$*% high watermark. The cache size is *$tmnxBsxDnsIpCacheSize$*.
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.

4.11 tmnxBsxDnsIpCacheFullClear

Table 26: 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
Source stream	main
Message format string	The usage of ISA-AA Group *$tmnxBsxIsaAaGroupIndex$* DNS IP Cache " *$tmnxBsxDnsIpCacheName$*" for ISA-MDA *$tmnxBsxNotify IsaMdaNum$* is less than or equal to the *$tmnxBsxDnsIpCacheLow Watermark$*% low watermark. The cache size is *$tmnxBsxDnsIpCache Size$*.
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 tmnxBsx DnsIpCacheSize 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.

4.12 tmnxBsxHttpUrlParamLimitExceeded

Table 27: 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
Source stream	main

Property name	Value
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.

4.13 tmnxBsxIsaAaGrpBitRate

Table 28: 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
Source stream	main
Message format string	Bit rate is greater than or equal to *$tmnxBsxBitRateHighWatermark$* megabits/s on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$*.
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.

4.14 tmnxBsxIsaAaGrpBitRateClear

Table 29: 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
Source stream	main
Message format string	Bit rate is less than or equal to *$tmnxBsxBitRateLowWatermark $* megabits/s on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* 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-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.

4.15 tmnxBsxIsaAaGrpCapCostThres

Table 30: tmnxBsxIsaAaGrpCapCostThres properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4409
Event name	tmnxBsxIsaAaGrpCapCostThres

Property name	Value
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.9
Default severity	warning
Source stream	main
Message format string	The capacity cost on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* 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.

4.16 tmnxBsxIsaAaGrpCapCostThresClear

Table 31: 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
Source stream	main
Message format string	The capacity cost on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* 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

Property name	Value
	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.

4.17 tmnxBsxIsaAaGrpFailureClearV2

Table 32: 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
Source stream	main
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.

4.18 tmnxBsxIsaAaGrpFailureV2

Table 33: tmnxBsxIsaAaGrpFailureV2 properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4401
Event name	tmnxBsxIsaAaGrpFailureV2

Property name	Value
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.5
Default severity	major
Source stream	main
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.

4.19 tmnxBsxIsaAaGrpFlowFull

Table 34: 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
Source stream	main
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* flow record usage is greater than or equal to high watermark. The Active ISA-AA MDA is *$tmnxBsxNotifyIsaMdaNum$*
Cause	Excessive traffic including denial of service attacks that target flow state exhaustion
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.

4.20 tmnxBsxIsaAaGrpFlowFullClear

Table 35: 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
Source stream	main
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* flow record usage is less than or equal to low watermark. The Active ISA-AA MDA is *$tmnx BsxNotifyIsaMdaNum$*
Cause	The conditions that caused tmnxBsxIsaAaGrpFlowFull or tmnxBsxIsa AaGrpFlowFull have been alleviated.
Effect	None.
Recovery	No recovery is required.

4.21 tmnxBsxIsaAaGrpFlowSetup

Table 36: 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
Source stream	main

Property name	Value
Message format string	Flow setup rate is greater than or equal to *$tmnxBsxFlowSetupHigh Watermark$* flows/s on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$*.
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.

4.22 tmnxBsxIsaAaGrpFlowSetupClear

Table 37: 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
Source stream	main
Message format string	Flow setup rate is less than or equal to *$tmnxBsxFlowSetupLow Watermark$* flows/s on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* 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.

4.23 tmnxBsxIsaAaGrpFmSbWaSBufOvld

Table 38: 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
Source stream	main
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.

4.24 tmnxBsxIsaAaGrpFmSbWaSBufOvldClr

Table 39: 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

Property name	Value
Default severity	warning
Source stream	main
Message format string	ISA-AA group *$tmnxBsxIsaAaGroupIndex$* MDA *$tmnxBsxNotify ActiveMda$* wa-shared buffer use is less than or equal to *$tmnxBsx IsaAaGrpFromSubWaSBfLoWmk$* in the from-subscriber direction or corresponding tmnxBsxIsaAaGrpFmSbWaSBufOvld notification has been disabled.
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.

4.25 tmnxBsxIsaAaGrpNonRedundantV2

Table 40: 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
Source stream	main
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.

Property name	Value
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.

4.26 tmnxBsxIsaAaGrpOvrldCutthru

Table 41: 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
Source stream	main
Message format string	ISA AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* MDA *$tmnxBsxNotifyIsaMdaNum$* 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.

4.27 tmnxBsxIsaAaGrpOvrldCutthruClr

Table 42: tmnxBsxIsaAaGrpOvrldCutthruClr properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4433

Property name	Value
Event name	tmnxBsxIsaAaGrpOvrldCutthruClr
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.33
Default severity	warning
Source stream	main
Message format string	ISA AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* MDA *$tmnxBsxNotifyIsaMdaNum$* 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.

4.28 tmnxBsxIsaAaGrpPacketRate

Table 43: 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
Source stream	main
Message format string	Packet rate is greater than or equal to *$tmnxBsxPacketRateHighWatermark$* packets/s on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$*.
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.

4.29 tmnxBsxIsaAaGrpPacketRateClear

Table 44: 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
Source stream	main
Message format string	Packet rate is less than or equal to *$tmnxBsxPacketRateLow Watermark$* packets/s on ISA-AA MDA *$tmnxBsxNotifyIsaMdaNum$* or corresponding tmnxBsxIsaAaGrpPacketRate notification has been disabled.
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.

4.30 tmnxBsxIsaAaGrpSwitchover

Table 45: tmnxBsxIsaAaGrpSwitchover properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4404
Event name	tmnxBsxIsaAaGrpSwitchover

Property name	Value
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.2
Default severity	warning
Source stream	main
Message format string	ISA-AA Group *$tmnxBsxNotifyIsaAaGroupIndex$* has switched activity. The Active ISA-AA MDA is now *$tmnxBsxNotifyIsaMdaNum$*
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.

4.31 tmnxBsxIsaAaGrpToSbWaSBufOvld

Table 46: tmnxBsxIsaAaGrpToSbWaSBufOvld properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4430
Event name	tmnxBsxIsaAaGrpToSbWaSBufOvld
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.30
Default severity	warning
Source stream	main
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 tmnxBsxIsaAaGrpToSbWaSBufOvld 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.

4.32 tmnxBsxIsaAaGrpToSbWaSBufOvldClr

Table 47: tmnxBsxIsaAaGrpToSbWaSBufOvldClr properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4431
Event name	tmnxBsxIsaAaGrpToSbWaSBufOvldClr
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.31
Default severity	warning
Source stream	main
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 tmnxBsxIsaAaGrpToSbWaSBufOvld notification has been disabled.
Cause	A tmnxBsxIsaAaGrpToSbWaSBufOvldClr is generated to indicate a prior tmnxBsxIsaAaGrpToSbWaSBufOvld 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 tmnxBsxIsaAaGrpToSbWaSBufOvld notification has been disabled by raising the tmnxBsxIsaAaGrpToSubWaSBfHiWmk to maximum.
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.

4.33 tmnxBsxIsaAaSubLoadBalance

Table 48: tmnxBsxIsaAaSubLoadBalance properties

Property name	Value
Application name	APPLICATION_ASSURANCE

Property name	Value
Event ID	4408
Event name	tmnxBsxIsaAaSubLoadBalance
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.8
Default severity	warning
Source stream	main
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.

4.34 tmnxBsxIsaAaTimFileProcFailure

Table 49: 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
Source stream	main
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 tmnxBsxNotifyReason 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

Property name	Value
	in the BOF. If successive attempts to load the isa-aa.tim fail, please contact Nokia customer support.

4.35 tmnxBsxMobileSubModifyFailure

Table 50: 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
Source stream	main
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 mismatch has not occurred to allow the overrides to be applied appropriately.

4.36 tmnxBsxRadApFailure

Table 51: tmnxBsxRadApFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE

Property name	Value
Event ID	4437
Event name	tmnxBsxRadApFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.37
Default severity	warning
Source stream	main
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.

4.37 tmnxBsxRadApIntrmUpdateSkipped

Table 52: 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
Source stream	main
Message format string	Interim update interval, configured as *$tmnxBsxRadApIntrmUpdate Interval$* minutes, has been ignored.
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.

Property name	Value
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).

4.38 tmnxBsxRadApServOperStateChange

Table 53: 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
Source stream	main
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.

4.39 tmnxBsxStatFtrEnTcaThreshCrClear

Table 54: tmnxBsxStatFtrEnTcaThreshCrClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE

Property name	Value
Event ID	4456
Event name	tmnxBsxStatFtrEnTcaThreshCrClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.56
Default severity	minor
Source stream	main
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$ $tmnxBsxNotifyTcaCfgFilterType$* "*$tmnxBsxNotifyTcaCfgFilterName$*" 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.

4.40 tmnxBsxStatFtrEnTcaThreshCrossed

Table 55: 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
Source stream	main
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$ $tmnxBsxNotifyTcaCfgFilterType$* "*$tmnxBsxNotifyTcaCfgFilterName$*" entry *$tmnxBsxNotifyTcaFtrEnCfgEntryId$* in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).

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

4.41 tmnxBsxStatFtrTcaThreshCrClear

Table 56: 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
Source stream	main
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.

4.42 tmnxBsxStatFtrTcaThreshCrossed

Table 57: 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
Default severity	minor
Source stream	main
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.

4.43 tmnxBsxStatPolcrTcaThreshCrClear

Table 58: 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

Property name	Value
Default severity	minor
Source stream	main
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotify AaGrpPartIndex$* 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.

4.44 tmnxBsxStatPolcrTcaThreshCrossed

Table 59: 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
Source stream	main
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotify AaGrpPartIndex$* 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 tmnxBsxStatTcaPolcrCfg 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.

4.45 tmnxBsxStatTcaThreshCrossed

Table 60: 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
Source stream	main
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 greater than or equal to the value of tmnxBsxStatTcaCfgHiWmark 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.

4.46 tmnxBsxStatTcaThreshCrossedClear

Table 61: tmnxBsxStatTcaThreshCrossedClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4450

Property name	Value
Event name	tmnxBsxStatTcaThreshCrossedClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.50
Default severity	minor
Source stream	main
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$ $tmnxBsxNotifyTcaCfgType$* in the *$tmnxBsxNotifyTcaCfgDirection$* 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 tmnxBsxNotifyReason will identify the utilization.
Effect	The tmnxBsxStatTcaThreshCrossed notification is cleared.
Recovery	There is no recovery for this notification.

4.47 tmnxBsxSubModifyFailure

Table 62: tmnxBsxSubModifyFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4443
Event name	tmnxBsxSubModifyFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.43
Default severity	minor
Source stream	main
Message format string	Failed to *$tmnxBsxNotifySubFailedAction$* a subscriber in group *$tmnxBsxNotifyAaGrpPartIndex$* on ISA-MDA *$tmnxBsxNotifyIsaMdaNum$* 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

Property name	Value
	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.

4.48 tmnxBsxSubQuarantined

Table 63: tmnxBsxSubQuarantined properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4463
Event name	tmnxBsxSubQuarantined
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.63
Default severity	minor
Source stream	main
Message format string	*$tmnxBsxAaSubscriberType$* subscriber *$tmnxBsxAaSubscriber$* added to quarantine
Cause	A tmnxBsxSubQuarantined notification is generated when a subscriber enters quarantined state.
Effect	The subscriber traffic will be marked as 'best effort' and colored as 'exceed profile' which will cause early discards.
Recovery	The subscriber quarantine must be removed manually using the tools command.

4.49 tmnxBsxSubQuarantinedClear

Table 64: tmnxBsxSubQuarantinedClear properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4464
Event name	tmnxBsxSubQuarantinedClear
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.64
Default severity	minor
Source stream	main
Message format string	*$tmnxBsxAaSubscriberType$* subscriber *$tmnxBsxAaSubscriber$* removed from quarantine
Cause	A tmnxBsxSubQuarantined notification is generated when a subscriber exits quarantined state.
Effect	The tmnxBsxTcpValTcaCrossed notification is cleared.
Recovery	There is no recovery for this notification.

4.50 tmnxBsxTcpValTcaCrossed

Table 65: 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
Source stream	main
Message format string	Threshold Crossing Alert raised for ISA-AA Group *$tmnxBsxNotifyAaGrpPartIndex$* TCP validate " *$tmnxBsxNotifyTcpValTcaName$*" in the *$tmnxBsxNotifyTcaCfgDirection$* direction (*$tmnxBsxNotifyReason$*).

Property name	Value
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 tmnx BsxNotifyReason will identify the utilization.
Effect	There is no effect for this notification.
Recovery	There is no recovery for this notification.

4.51 tmnxBsxTcpValTcaCrossedClear

Table 66: 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
Source stream	main
Message format string	Threshold Crossing Alert cleared for ISA-AA Group *$tmnxBsxNotify AaGrpPartIndex$* 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 tmnxBsxNotify Reason will identify the utilization.
Effect	The tmnxBsxTcpValTcaCrossed notification is cleared.
Recovery	There is no recovery for this notification.

4.52 tmnxBsxTransIpPolAaSubCreated

Table 67: tmnxBsxTransIpPolAaSubCreated properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4421
Event name	tmnxBsxTransIpPolAaSubCreated
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.21
Default severity	warning
Source stream	main
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.

4.53 tmnxBsxTransIpPolAaSubDeleted

Table 68: 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
Source stream	main

Property name	Value
Message format string	A dynamic transit subscriber *$tmnxBsxNotifyAaSubscriberName$* has been deleted from group-partition *$tmnxBsxNotifyAaGrpPartIndex $* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$$tmnxBsxNotify Reason$*.
Cause	A tmnxBsxTransIpPolAaSubDeleted notification is generated when a dynamic subscriber is deleted in a Transit IP Policy.
Effect	None.
Recovery	No recovery is required.

4.54 tmnxBsxTransIpPolDhcpAddWarning

Table 69: 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
Source stream	main
Message format string	Problem encountered while attempting to add a transit subscriber to group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnx BsxNotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.
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.

4.55 tmnxBsxTransIpPolDhcpDelWarning

Table 70: 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
Source stream	main
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 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.

4.56 tmnxBsxTransIpPolDiamGxError

Table 71: 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

Property name	Value
Default severity	minor
Source stream	main
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.

4.57 tmnxBsxTransIpPolRadCoAAudit

Table 72: tmnxBsxTransIpPolRadCoAAudit properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4423
Event name	tmnxBsxTransIpPolRadCoAAudit
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.23
Default severity	warning
Source stream	main
Message format string	CoA audit for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* is in state *$tmnxBsxNotify RadiusCoAAuditState$*.
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.

4.58 tmnxBsxTransIpPolRadCoAError

Table 73: 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
Source stream	main
Message format string	Problem encountered while processing a CoA request for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsx NotifyTransitIpPolicyId$*: *$tmnxBsxNotifyReason$*.
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.

4.59 tmnxBsxTransIpPolRadDiscError

Table 74: 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

Property name	Value
Default severity	minor
Source stream	main
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 Disconnect 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.

4.60 tmnxBsxTransitIpPersistenceWarn

Table 75: 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
Source stream	main
Message format string	Problem encountered while registering transit subscriber address persistently for group-partition *$tmnxBsxNotifyAaGrpPartIndex$* transit IP policy *$tmnxBsxNotifyTransitIpPolicyId$* : *$tmnxBsxNotifyReason$*.
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.

Property name	Value
Recovery	No recovery is required.

4.61 tmnxBsxUrlFilterOperStateChange

Table 76: 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
Source stream	main
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.

4.62 tmnxBsxUrlFltrWebServOprStateChg

Table 77: tmnxBsxUrlFltrWebServOprStateChg properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4465
Event name	tmnxBsxUrlFltrWebServOprStateChg

Property name	Value
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.65
Default severity	minor
Source stream	main
Message format string	AA Group *$tmnxBsxIsaAaGroupIndex$* URL Filter *$tmnxBsxUrlFilterName$* DNS server state changed to *$tmnxBsxUrlFltrWebSvDnsOperState$*, flags = *$tmnxBsxUrlFltrWebSvDnsOperFlags$*.
Cause	The tmnxBsxUrlFltrWebServOprStateChg notification is generated when the operational status of a URL Filter Web Service DNS Server has transitioned either from 'inService' to 'outOfService' or from 'out OfService' to 'inService'.
Effect	N/A
Recovery	N/A

4.63 tmnxBsxUrlListFailure

Table 78: tmnxBsxUrlListFailure properties

Property name	Value
Application name	APPLICATION_ASSURANCE
Event ID	4447
Event name	tmnxBsxUrlListFailure
SNMP notification prefix and OID	TIMETRA-BSX-NG-MIB.tmnxBsxNotifications.47
Default severity	minor
Source stream	main
Message format string	URL list "*$tmnxBsxUrlListName$*" in ISA-AA group *$tmnxBsxIsaAaGroupIndex$* has failed. The current operational state is: *$tmnxBsxUrlListStatusOperState$*, 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.

Property name	Value
Recovery	The customer should ensure the correct file is configured in tmnxBsx UrlListFileUrl, and use tmnxBsxUrlListAdminState or tmnxBsxUrlList Upgrade to restart the URL List.

4.64 tmnxBsxUrlListUpdate

Table 79: 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
Source stream	main
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.

5 APS

5.1 apsEventChannelMismatch

Table 80: 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
Source stream	main
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.

5.2 apsEventFEPLF

Table 81: apsEventFEPLF properties

Property name	Value
Application name	APS
Event ID	2005
Event name	apsEventFEPLF

Property name	Value
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.5
Default severity	minor
Source stream	main
Message format string	FEPL failure is declared
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

5.3 apsEventModeMismatch

Table 82: 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
Source stream	main
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 unidirectional. 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).

5.4 apsEventPSBF

Table 83: apsEventPSBF properties

Property name	Value
Application name	APS
Event ID	2004
Event name	apsEventPSBF
SNMP notification prefix and OID	APS-MIB.apsNotificationsPrefix.4
Default severity	minor
Source stream	main
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.

5.5 apsEventSwitchover

Table 84: 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
Source stream	main
Message format string	APS switchover from *$subject$*.

Property name	Value
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.

5.6 tApsChannelMismatchClear

Table 85: 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
Source stream	main
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

5.7 tApsChanTxLaisStateChange

Table 86: tApsChanTxLaisStateChange properties

Property name	Value
Application name	APS

Property name	Value
Event ID	2015
Event name	tApsChanTxLaisStateChange
SNMP notification prefix and OID	TIMETRA-APS-MIB.tApsNotifications.10
Default severity	warning
Source stream	main
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.

5.8 tApsFEPLFClear

Table 87: 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
Source stream	main
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

5.9 tApsLocalSwitchCommandClear

Table 88: 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
Source stream	main
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

5.10 tApsLocalSwitchCommandSet

Table 89: 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

Property name	Value
Source stream	main
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

5.11 tApsMcApsCtlLinkStateChange

Table 90: 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
Source stream	main
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
Recovery	Investigation is required to determine the cause of the change.

5.12 tApsModeMismatchClear

Table 91: 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
Source stream	main
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

5.13 tApsPrimaryChannelChange

Table 92: 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
Source stream	main
Message format string	Switch of the primary APS channel to *$apsStatusK1K2Trans$*.
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

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

5.14 tApsPSBFClear

Table 93: 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
Source stream	main
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

5.15 tApsRemoteSwitchCommandClear

Table 94: 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
Source stream	main
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

5.16 tApsRemoteSwitchCommandSet

Table 95: 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
Source stream	main
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.

6 AUTO_PROV

6.1 autoNodeProv

Table 96: autoNodeProv properties

Property name	Value
Application name	AUTO_PROV
Event ID	2001
Event name	autoNodeProv
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	*$subject$*: *$title$* *$message$*
Cause	The system generated an auto-node-provision message.
Effect	Unknown.
Recovery	Contact Nokia customer service.

7 BFD

7.1 tmnxBfdOnLspExtSessDeleted

Table 97: tmnxBfdOnLspExtSessDeleted properties

Property name	Value
Application name	BFD
Event ID	2009
Event name	tmnxBfdOnLspExtSessDeleted
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.9
Default severity	minor
Source stream	main
Message format string	The *$tmnxBfdOnLspExtSessLinkType$* BFD Session with Local Discriminator *$tmnxBfdOnLspExtSessLclDisc$* on *$subject$* has been deleted
Cause	The tmnxBfdOnLspExtSessDeleted 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.

7.2 tmnxBfdOnLspExtSessDown

Table 98: tmnxBfdOnLspExtSessDown properties

Property name	Value
Application name	BFD
Event ID	2007

Property name	Value
Event name	tmnxBfdOnLspExtSessDown
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.7
Default severity	minor
Source stream	main
Message format string	The *$tmnxBfdOnLspExtSessLinkType$* BFD session with Local Discriminator *$tmnxBfdOnLspExtSessLclDisc$* on *$subject$* is down due to *$tmnxBfdOnLspExtSessOperFlags$*
Cause	The tmnxBfdOnLspExtSessDown 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 its own.

7.3 tmnxBfdOnLspExtSessNoCpmNpResrcs

Table 99: tmnxBfdOnLspExtSessNoCpmNpResrcs properties

Property name	Value
Application name	BFD
Event ID	2011
Event name	tmnxBfdOnLspExtSessNoCpmNpResrcs
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.11
Default severity	minor
Source stream	main
Message format string	The *$tmnxBfdOnLspExtSessLinkType$* BFD session with local discriminator *$tmnxBfdOnLspExtSessLclDisc$* on *$subject$* could not be established because cpm-np session termination resources are not available
Cause	The tmnxBfdOnLspExtSessNoCpmNpResrcs notification is generated when a BFD on LSP session could not be established because the session requires a cpmNp or fp session termination resource (see

Property name	Value
	TIMETRA-VRTR-MIB::vRtrIfBfdExtType), and no cpmNp or fp session termination resources are available.
Effect	The BFD session cannot be established until a cpmNp or fp session termination resource is available
Recovery	There is no recovery required for this notification.

7.4 tmnxBfdOnLspExtSessProtChange

Table 100: tmnxBfdOnLspExtSessProtChange properties

Property name	Value
Application name	BFD
Event ID	2010
Event name	tmnxBfdOnLspExtSessProtChange
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.10
Default severity	minor
Source stream	main
Message format string	The protocol (*$tmnxBfdOnLspExtSessChngdProtocol$*) using BFD session on node *$subject$* has been *$tmnxBfdOnLspExtSessProto ChngdSta$*
Cause	The tmnxBfdOnLspExtSessProtChange notification is generated when there is a change in the list of protocols specified by tmnxBfdOnLspExt 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.

7.5 tmnxBfdOnLspExtSessUp

Table 101: tmnxBfdOnLspExtSessUp properties

Property name	Value
Application name	BFD
Event ID	2008
Event name	tmnxBfdOnLspExtSessUp
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.8
Default severity	minor
Source stream	main
Message format string	The *$tmnxBfdOnLspExtSessLinkType$* BFD session with Local Discriminator *$tmnxBfdOnLspExtSessLclDisc$* on *$subject$* is up
Cause	The tmnxBfdOnLspExtSessUp notification is generated when a BFD on LSP session goes up.
Effect	The BFD session will be active.
Recovery	There is no recovery required for this notification.

7.6 tmnxBfdOnLspSessDeleted

Table 102: 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
Source stream	main
Message format string	The *$tmnxBfdOnLspSessLinkType$* BFD Session with Local Discriminator *$tmnxBfdOnLspSessLclDisc$* on *$subject$* has been deleted

Property name	Value
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.

7.7 tmnxBfdOnLspSessDown

Table 103: 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
Source stream	main
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 its own.

7.8 tmnxBfdOnLspSessNoCpmNpResources

Table 104: 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
Source stream	main
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 or fp session termination resource (see TIMETRA-VRTR-MIB::vRtrIfBfdExtType), and no cpmNp or fp session termination resources are available.
Effect	The BFD session cannot be established until a cpmNp or fp session termination resource is available
Recovery	There is no recovery required for this notification.

7.9 tmnxBfdOnLspSessNoTailResources

Table 105: tmnxBfdOnLspSessNoTailResources properties

Property name	Value
Application name	BFD
Event ID	2006
Event name	tmnxBfdOnLspSessNoTailResources
SNMP notification prefix and OID	TIMETRA-BFD-MIB.tmnxBfdNotifications.6
Default severity	minor
Source stream	main

Property name	Value
Message format string	BFD on LSP session(s) could not be established because BFD on LSP session tail-end creation is administratively disabled, or the limit on the number of BFD on LSP session tail-ends has been reached (admin state = *$vRtrLspBfdSession$*, limit = *$vRtrLspBfdMaxSessions$*)
Cause	The tmnxBfdOnLspSessNoTailResources notification is generated when a BFD on LSP session could not be established by the LSP's tail-end system because the system limit on the number of session tail ends has been reached. If TIMETRA-VRTR-MIB::vRtrLspBfdSession is 'enabled(1)', the system limit on the number of session tail ends is TIMETRA-VRTR-MIB::vRtrLspBfdMaxSessions. If TIMETRA-VRTR-MIB::vRtrLspBfdSession is 'disabled(2)', the system limit on the number of session tail ends is zero. This notification is throttled using the following mechanism. In the initial state (e.g. at CPM startup), when the first failure is detected, tmnxBfdOnLspSessNoTailResources is raised, and a ten minute timer is started. When the timer expires, 1. tmnxBfd OnLspSessNoTailResources is raised if one or more failures occurred in the ten minute interval, and 2. A ten minute timer is started (and the process repeats). Any change to TIMETRA-VRTR-MIB::vRtrLspBfd Session and/or TIMETRA-VRTR-MIB::vRtrLspBfdMaxSessions restarts the process at the initial state.
Effect	One or more BFD on LSP sessions could not be established.
Recovery	Change TIMETRA-VRTR-MIB::vRtrLspBfdSession to 'enabled(1)', or increase TIMETRA-VRTR-MIB::vRtrLspBfdMaxSessions, or change the network configuration to reduce the number of active BFD on LSP session tail ends.

7.10 tmnxBfdOnLspSessProtChange

Table 106: 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
Source stream	main

Property name	Value
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.

7.11 tmnxBfdOnLspSessUp

Table 107: 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
Source stream	main
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.
Recovery	There is no recovery required for this notification.

8 BGP

8.1 bgpBackwardTransNotification

Table 108: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *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

8.2 bgpCfgViol

Table 109: bgpCfgViol properties

Property name	Value
Application name	BGP
Event ID	2017

Property name	Value
Event name	bgpCfgViol
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	*$subject$*: BGP - *$field$* configuration ignored - *$reason$*
Cause	BGP configuration was invalid.
Effect	The configuration that led to the violation will be totally ignored.
Recovery	N/A

8.3 bgpConnMgrTerminated

Table 110: bgpConnMgrTerminated properties

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

8.4 bgpConnNoKA

Table 111: bgpConnNoKA properties

Property name	Value
Application name	BGP
Event ID	2008
Event name	bgpConnNoKA
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: closing inbound connection because the BGP peer did not receive "keepalive"
Cause	A BGP KEEPALIVE message was not received within the hold-time limit.
Effect	Inbound connection failed to establish.
Recovery	Reset and try again.

8.5 bgpConnNoOpenRcvd

Table 112: bgpConnNoOpenRcvd properties

Property name	Value
Application name	BGP
Event ID	2009
Event name	bgpConnNoOpenRcvd
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: closing inbound connection because the BGP peer did not receive "open"
Cause	A BGP OPEN message was not received within the hold-time limit.
Effect	Inbound connection failed to establish.

Property name	Value
Recovery	Reset and try again.

8.6 bgpEstablishedNotification

Table 113: bgpEstablishedNotification properties

Property name	Value
Application name	BGP
Event ID	2038
Event name	bgpEstablishedNotification
SNMP notification prefix and OID	BGP4-MIB.bgpNotification.1
Default severity	minor
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *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

8.7 bgpInterfaceDown

Table 114: bgpInterfaceDown properties

Property name	Value
Application name	BGP
Event ID	2007
Event name	bgpInterfaceDown

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *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.

8.8 bgpNoMemoryPeer

Table 115: bgpNoMemoryPeer properties

Property name	Value
Application name	BGP
Event ID	2015
Event name	bgpNoMemoryPeer
SNMP notification prefix and OID	N/A
Default severity	critical
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *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.

8.9 bgpPeerNotFound

Table 116: bgpPeerNotFound properties

Property name	Value
Application name	BGP
Event ID	2012
Event name	bgpPeerNotFound
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *$subject$*: 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.

8.10 bgpRejectConnBadLocAddr

Table 117: bgpRejectConnBadLocAddr properties

Property name	Value
Application name	BGP
Event ID	2010
Event name	bgpRejectConnBadLocAddr
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main

Property name	Value
Message format string	(ASN *$tBgpASN4Byte$*) *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; for example, the one mentioned in the local-address of the local peer.

8.11 bgpRemoteEndClosedConn

Table 118: bgpRemoteEndClosedConn properties

Property name	Value
Application name	BGP
Event ID	2011
Event name	bgpRemoteEndClosedConn
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *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 learned from that peer were rejected.
Recovery	Reset and try to re-establish the peering.

8.12 bgpTerminated

Table 119: bgpTerminated properties

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

8.13 bgpVariableRangeViolation

Table 120: bgpVariableRangeViolation properties

Property name	Value
Application name	BGP
Event ID	2016
Event name	bgpVariableRangeViolation
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
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 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

Property name	Value
	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 Nokia BGP MIB.
Effect	The set value is not accepted but the closest valid value to the set value is accepted.
Recovery	N/A

8.14 receiveNotification

Table 121: receiveNotification properties

Property name	Value
Application name	BGP
Event ID	2006
Event name	receiveNotification
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: received notification: code *$code_str$* subcode *$subcode_str$*
Cause	Any error that occurred between BGP peers that was first recognized by the remote BGP instance. e.g. 1) An error occurred in the state transitions of a peering session. 2) An error occurred 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

8.15 sendNotification

Table 122: sendNotification properties

Property name	Value
Application name	BGP
Event ID	2005
Event name	sendNotification
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: sending notification: code *$code_str$* subcode *$subcode_str$*
Cause	Any error that occurred between BGP peers that was first recognized by the local BGP instance. e.g. 1) An error occurred in the state transitions of a peering session. 2) An error occurred 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

8.16 tBgp4PathAttrDiscarded

Table 123: tBgp4PathAttrDiscarded properties

Property name	Value
Application name	BGP
Event ID	2040
Event name	tBgp4PathAttrDiscarded
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.24
Default severity	warning
Source stream	main

Property name	Value
Message format string	(ASN *$tBgpASN4Byte$*) *$vRtrID$*: Discarded path attribute received from BGP Peer *$tBgpPeerNgAddr$* with attribute type [*$tBgp4PathAttrType$*] and length [*$tBgp4PathAttrLength$*]. Hex dump: *$tBgp4PathAttribute$*
Cause	The tBgp4PathAttrDiscarded notification is generated when a path attribute tBgp4PathAttribute is discarded from an UPDATE message. A path attribute may be discarded because it is malformed.
Effect	A log entry is generated for each path attribute discarded from an UPDATE message. The UPDATE message continues to be processed.
Recovery	There is no recovery required for this notification.

8.17 tBgp4PathAttrInvalid

Table 124: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *$vRtrID$*: BGP Peer *$tBgpPeerNgAddr$*: Invalid path attribute received with attribute type [*$tBgp4PathAttrType$*] and length [*$tBgp4PathAttrLength$*]. Hex dump: *$tBgp4PathAttribute$*
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.

8.18 tBgp4RouteInvalid

Table 125: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *$vRtrID$*: 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 cannot 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.

8.19 tBgp4UpdateInvalid

Table 126: tBgp4UpdateInvalid properties

Property name	Value
Application name	BGP
Event ID	2030
Event name	tBgp4UpdateInvalid

Property name	Value
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.18
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *$vRtrID$*: 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.

8.20 tBgp4WithdrawnRtFromUpdateError

Table 127: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *$vRtrID$*: 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.

8.21 tBgpFibResourceFailPeer

Table 128: tBgpFibResourceFailPeer properties

Property name	Value
Application name	BGP
Event ID	2032
Event name	tBgpFibResourceFailPeer
SNMP notification prefix and OID	N/A
Default severity	critical
Source stream	main
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.

8.22 tBgpFlowspecUnsupportdComAction

Table 129: 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
Source stream	main

Property name	Value
Message format string	(ASN *$tBgpASN4Byte$*) *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 does not create an 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.

8.23 tBgpGeneral

Table 130: tBgpGeneral properties

Property name	Value
Application name	BGP
Event ID	2031
Event name	tBgpGeneral
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
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.

8.24 tBgpInstanceDynamicPeerLmtReachd

Table 131: 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
Source stream	main
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.

8.25 tBgpInstConvStateTransition

Table 132: tBgpInstConvStateTransition properties

Property name	Value
Application name	BGP
Event ID	2042
Event name	tBgpInstConvStateTransition
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.25
Default severity	minor

Property name	Value
Source stream	main
Message format string	Convergence state for family *$tBgpConvergenceFamily$* transitioned from *$tBgpOldConvergenceState$* to *$tBgpConvergenceState$*
Cause	The tBgpInstConvStateTransition notification is generated when the convergence state transitions.
Effect	A log entry is generated.
Recovery	There is no recovery required for this notification.

8.26 tBgpMaxNgPfxLmt

Table 133: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: number of routes learned has exceeded configured maximum (*$tBgpPeerNgPfxLmtMaxPrefix$*) for *$tBgpPeerNgPfxLmtFamily$* 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.

8.27 tBgpMaxNgPfxLmtThresholdReached

Table 134: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: number of routes learned has exceeded *$tBgpPeerNgPfxLmtThreshold$* percentage of the configured maximum (*$tBgpPeerNgPfxLmtMaxPrefix$*) for *$tBgpPeer NgPfxLmtFamily$* family
Cause	A tBgpMaxNgPfxLmtThresholdReached notification is generated when the number of routes learned from the peer has exceeded tBgpPeer 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.

8.28 tBgpNgBackwardTransition

Table 135: 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
Source stream	main

Property name	Value
Message format string	(ASN *$tBgpASN4Byte$*) *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

8.29 tBgpNgEstablished

Table 136: tBgpNgEstablished properties

Property name	Value
Application name	BGP
Event ID	2019
Event name	tBgpNgEstablished
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.7
Default severity	minor
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *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

8.30 tBgpPeerGRStatusChange

Table 137: 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
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: graceful restart status changed to *$tBgpPeerNgOperGRStatus$*
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

8.31 tBgpPeerNgGRStatusChange

Table 138: tBgpPeerNgGRStatusChange properties

Property name	Value
Application name	BGP
Event ID	2043
Event name	tBgpPeerNgGRStatusChange
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.6
Default severity	minor
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: graceful restart status changed to *$tBgpPeerNgOperGRStatus$*
Cause	The BGP peer is either restarting or just changed the graceful restart status to 'helping'/'not helping'/'restart complete'.

Property name	Value
Effect	N/A
Recovery	N/A

8.32 tBgpPeerNgHoldTimeInconsistent

Table 139: tBgpPeerNgHoldTimeInconsistent properties

Property name	Value
Application name	BGP
Event ID	2021
Event name	tBgpPeerNgHoldTimeInconsistent
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.9
Default severity	warning
Source stream	main
Message format string	(ASN *$tBgpASN4Byte$*) *bgp_peer_name*: attempted to negotiate a hold timer lower than the configured minimum value of *$tBgpPeer NgMinHoldTime$*
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.

8.33 tBgpPGDynamicPeerLmtReached

Table 140: tBgpPGDynamicPeerLmtReached properties

Property name	Value
Application name	BGP
Event ID	2037

Property name	Value
Event name	tBgpPGDynamicPeerLmtReached
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.23
Default severity	minor
Source stream	main
Message format string	*bgp_peer_name*: Closing connection: reached dynamic peer limit (*$tBgpPGDynamicPeerLimit$*) for BGP group *$tBgpPeerGroupName$*
Cause	A tBgpPGDynamicPeerLmtReached notification is generated 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.

8.34 tBgpPGDynNbrIfMaxSessLmtReachd

Table 141: tBgpPGDynNbrIfMaxSessLmtReachd properties

Property name	Value
Application name	BGP
Event ID	2044
Event name	tBgpPGDynNbrIfMaxSessLmtReachd
SNMP notification prefix and OID	TIMETRA-BGP-MIB.tBgpNotifications.26
Default severity	minor
Source stream	main
Message format string	*bgp_peer_name*: Closing connection: reached max sessions limit (*$tBgpPGDynNbrIfMaxSessions$*) for interface *$tBgpPGDynNbrInterfaceIndex$*
Cause	The tBgpPGDynNbrIfMaxSessLmtReachd notification is generated when the dynamic session limit for this interface is reached.
Effect	Whenever an incoming connection for a new dynamic session would cause dynamic session limit for this interface to be exceeded, the connection attempt is rejected.

Property name	Value
Recovery	Increase the dynamic peer limit for this interface.

8.35 tBgpReceivedInvalidNlri

Table 142: 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
Source stream	main
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.

8.36 tmnxBmpSessionStatusChange

Table 143: tmnxBmpSessionStatusChange properties

Property name	Value
Application name	BGP
Event ID	2041
Event name	tmnxBmpSessionStatusChange

Property name	Value
SNMP notification prefix and OID	TIMETRA-BMP-MIB.tmnxBmpNotifications.1
Default severity	minor
Source stream	main
Message format string	VR *$tmnxBmpSessionChangeVRtrID$*: Station *$tmnxBmpSessionChangeStationName$* moved from state *$tmnxBmpSessionChangeOldState$* to state *$tmnxBmpSessionChangeNewState$* due to reason: *$tmnxBmpSessionChangeReason$*
Cause	The tmnxBmpSessionStatusChange notification is generated when a BMP session has changed its status.
Effect	This notification has no direct effect. The old and new connection states and the change reason are logged to aid debugging and tracking back the root cause of the problem.
Recovery	There is no recovery required for this notification.

9 BIER

9.1 vRtrBierBfrIdCollision

Table 144: vRtrBierBfrIdCollision properties

Property name	Value
Application name	BIER
Event ID	2001
Event name	vRtrBierBfrIdCollision
SNMP notification prefix and OID	TIMETRA-BIER-MIB.vRtrBierNotifications.1
Default severity	minor
Source stream	main
Message format string	Same BFR id *$vRtrBierNotifyBfrId$* received from *$vRtrBier Prefix1Address$* and *$vRtrBierPrefix2Address$* by the sub-domain *$v RtrBierNotifySubDomainId$* with BSL *$vRtrBierNotifyBsl$*
Cause	The vRtrBierBfrIdCollision is generated when BFR ID received from two different routes is the same.
Effect	We will remove the duplicate BFR Id from neighbors f-BM (forwarding Bit Mask).
Recovery	An operator intervention is needed to remove the duplicate BFR ID from the configuration.

9.2 vRtrBierMtMismatch

Table 145: vRtrBierMtMismatch properties

Property name	Value
Application name	BIER
Event ID	2002

Property name	Value
Event name	vRtrBierMtMismatch
SNMP notification prefix and OID	TIMETRA-BIER-MIB.vRtrBierNotifications.2
Default severity	minor
Source stream	main
Message format string	Multi-topology value *$vRtrBierNotifyRecvMTId$* received by the sub-domain *$vRtrBierNotifySubDomainId$* with BSL *$vRtrBierNotifyBsl$* and multi-topology *$vRtrBierNotifyMTId$*
Cause	The vRtrBierMtMismatch is generated when the multi- topology sent by the peer is different from what is configured locally.
Effect	We will ignore the advertisement.
Recovery	N/A

9.3 vRtrBierSubDomainMismatch

Table 146: vRtrBierSubDomainMismatch properties

Property name	Value
Application name	BIER
Event ID	2003
Event name	vRtrBierSubDomainMismatch
SNMP notification prefix and OID	TIMETRA-BIER-MIB.vRtrBierNotifications.3
Default severity	minor
Source stream	main
Message format string	Sub-domain value *$vRtrBierNotifyRecvSubDomainId$* received by the sub-domain *$vRtrBierNotifySubDomainId$* with BSL *$vRtrBierNotifyBsl$*
Cause	The vRtrBierSubDomainMismatch is generated when the sub-domain in the received route is not configured locally.
Effect	We will ignore the sub TLV.
Recovery	Operator may need to configure the mismatched sub-domains.

9.4 vRtrBierUnsupportedNhop

Table 147: vRtrBierUnsupportedNhop properties

Property name	Value
Application name	BIER
Event ID	2004
Event name	vRtrBierUnsupportedNhop
SNMP notification prefix and OID	TIMETRA-BIER-MIB.vRtrBierNotifications.4
Default severity	minor
Source stream	main
Message format string	Next-hop type *$vRtrBierNextHopeType$* is not supported for the given prefix *$vRtrBierPrefix1Address$*, next-hop address *$vRtrBierNextHop Address$* and outgoing interface *$vRtrIfIndex$*
Cause	The vRtrBierUnsupportedNhop is generated when the next hop indicated by vRtrBierNextHopAddress is unsupported by the system.
Effect	We will ignore it while calculating the next hop.
Recovery	The recovery is caused on receiving the subsequent correct next hop and clearing this trap by setting vRtrBierUnsupportedNhopState to 'false'.

10 CALLTRACE

10.1 calltraceDebugEvent

Table 148: calltraceDebugEvent properties

Property name	Value
Application name	CALLTRACE
Event ID	2003
Event name	calltraceDebugEvent
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	debug
Message format string	*$subject$*: *$title$* *$message$*
Cause	Call trace generated a debug message because calltrace debugging was enabled. The event may show a packet or an event related to the sessions being traced in the system.
Effect	None.
Recovery	Disable calltrace debugging to stop receiving the event.

10.2 tmnxCallTraceLocSizeLimitReached

Table 149: tmnxCallTraceLocSizeLimitReached properties

Property name	Value
Application name	CALLTRACE
Event ID	2002

Property name	Value
Event name	tmnxCallTraceLocSizeLimitReached
SNMP notification prefix and OID	TIMETRA-CALLTRACE-MIB.tmnxCallTraceNotifications.2
Default severity	minor
Source stream	main
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.

10.3 tmnxCallTraceMaxFilesNumReached

Table 150: tmnxCallTraceMaxFilesNumReached properties

Property name	Value
Application name	CALLTRACE
Event ID	2001
Event name	tmnxCallTraceMaxFilesNumReached
SNMP notification prefix and OID	TIMETRA-CALLTRACE-MIB.tmnxCallTraceNotifications.1
Default severity	minor
Source stream	main
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.

Property name	Value
	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.

11 CFLOWD

11.1 tmnxCflowdCreateFailure

Table 151: 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
Source stream	main
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.

11.2 tmnxCflowdFlowCreateFailure

Table 152: tmnxCflowdFlowCreateFailure properties

Property name	Value
Application name	CFLOWD
Event ID	2006
Event name	tmnxCflowdFlowCreateFailure
SNMP notification prefix and OID	TIMETRA-CFLOWD-MIB.tmnxCflowdNotifications.6

Property name	Value
Default severity	minor
Source stream	main
Message format string	Cflowd flow creation failed - *$tmnxCflowdFlowFailureReasonCode$*
Cause	The tmnxCflowdFlowCreateFailure event is generated when the creation of a cflowd flow fails.
Effect	Flow data may be lost.
Recovery	N/A

11.3 tmnxCflowdPacketTxFailure

Table 153: 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
Source stream	main
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

11.4 tmnxCflowdStateChange

Table 154: tmnxCflowdStateChange properties

Property name	Value
Application name	CFLOWD
Event ID	2004
Event name	tmnxCflowdStateChange
SNMP notification prefix and OID	TIMETRA-CFLOWD-MIB.tmnxCflowdNotifications.4
Default severity	minor
Source stream	main
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

12 CHASSIS

12.1 CpmIcPortSFFStatusDDMCorrupt

Table 155: 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
Source stream	main
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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.2 CpmIcPortSFFStatusFailure

Table 156: CpmIcPortSFFStatusFailure properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	4011
Event name	CpmIcPortSFFStatusFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.7
Default severity	minor
Source stream	main
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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.3 CpmIcPortSFFStatusReadError

Table 157: 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
Source stream	main
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)'.

Property name	Value
Effect	The SFF device is not operational and the associated CPM interconnect port cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.4 CpmIcPortSFFStatusUnsupported

Table 158: 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
Source stream	main
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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.5 SfmIcPortSFFStatusDDMCorrupt

Table 159: 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
Source stream	main
Message format string	SFM interconnect port SFF DDM 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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.6 SfmIcPortSFFStatusFailure

Table 160: 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
Source stream	main

Property name	Value
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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.7 SfmIcPortSFFStatusReadError

Table 161: 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
Source stream	main
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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.8 SfmIcPortSFFStatusUnsupported

Table 162: 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
Source stream	main
Message format string	SFM interconnect port SFF unsupported type
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 cannot be used. The SFF and port will not recover without operator intervention.
Recovery	Remove and reinsert the SFF device. If the problem persists then replace the SFF device.

12.9 tChassisAirflowDirMismatch

Table 163: tChassisAirflowDirMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2233
Event name	tChassisAirflowDirMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.244

Property name	Value
Default severity	critical
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: airflow direction mismatch
Cause	The tChassisAirflowDirMismatch notification is generated when airflow direction is not identical for all chassis fans and power-supply fans equipped by the physical chassis.
Effect	Mismatched airflow direction among fans may cause increased temperature, intermittent errors, and could damage components.
Recovery	The operator must identify a single preferred airflow direction, remove any chassis fans and power-supply fans which do not match it, and replace them with equipment having fans of the preferred airflow direction.

12.10 tChassisAirflowDirMismatchClr

Table 164: tChassisAirflowDirMismatchClr properties

Property name	Value
Application name	CHASSIS
Event ID	2234
Event name	tChassisAirflowDirMismatchClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.245
Default severity	critical
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: airflow direction mismatch cleared
Cause	The tChassisAirflowDirMismatchClr notification is generated to indicate that all chassis fans and power-supply fans with mismatched airflow directions have been replaced, and all chassis-fans and power-supply fans share the same direction.
Effect	N/A
Recovery	N/A

12.11 tChassisPowerSupplyMismatch

Table 165: tChassisPowerSupplyMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2235
Event name	tChassisPowerSupplyMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.246
Default severity	critical
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: power-supply type mismatch
Cause	The tChassisPowerSupplyMismatch notification is generated when power-supply elements equipped to the physical chassis are not all of the same type.
Effect	There is an increased risk of power-supply failure. Intermittent error or damage to components may also result.
Recovery	The operator must identify a single preferred or required power-supply type, remove any power-supply elements of other types, and replace them with equipment of the preferred power-supply type.

12.12 tChassisPowerSupplyMismatchClr

Table 166: tChassisPowerSupplyMismatchClr properties

Property name	Value
Application name	CHASSIS
Event ID	2236
Event name	tChassisPowerSupplyMismatchClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.247

Property name	Value
Default severity	critical
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: power-supply type mismatch cleared
Cause	The tChassisPowerSupplyMismatchClr notification is generated to indicate that all power-supply elements of mismatched types have been replaced, and all power-supply elements now share the same type.
Effect	N/A
Recovery	N/A

12.13 tChassisPowerSupplyUnsup

Table 167: tChassisPowerSupplyUnsup properties

Property name	Value
Application name	CHASSIS
Event ID	2237
Event name	tChassisPowerSupplyUnsup
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.248
Default severity	critical
Source stream	main
Message format string	*$tmnxChassisNotifyHwIndex$*: power-supply not supported
Cause	The tChassisPowerSupplyUnsup notification is generated when power-supply elements equipped to the physical chassis are not of a supported type.
Effect	There is an increased risk of power-supply failure. Intermittent error or damage to components may also result.
Recovery	The operator must identify any equipped power supply elements of unsupported type, remove them, and replace them with equipment of a supported power-supply type

12.14 tIPsecEsaVmMemHighWatermark

Table 168: tIPsecEsaVmMemHighWatermark properties

Property name	Value
Application name	CHASSIS
Event ID	2220
Event name	tIPsecEsaVmMemHighWatermark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.231
Default severity	minor
Source stream	main
Message format string	The memory usage ratio for ESA-VM *$tmnxEsaNotifyId$*/*$tmnxEsaVmNotifyId$* has almost reached the maximum value.
Cause	A tIPsecEsaVmMemHighWatermark notification is generated when the ESA VM 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.

12.15 tIPsecEsaVmMemLowWatermark

Table 169: tIPsecEsaVmMemLowWatermark properties

Property name	Value
Application name	CHASSIS
Event ID	2219
Event name	tIPsecEsaVmMemLowWatermark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.230
Default severity	minor
Source stream	main

Property name	Value
Message format string	The memory usage ratio for ESA-VM *$tmnxEsaNotifyId$*/*$tmnxEsa VmNotifyId$* has dropped back to the normal level.
Cause	A tIPsecEsaVmMemLowWatermark notification is generated when the ESA VM 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.

12.16 tIPsecIsaMemHighWatermark

Table 170: 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
Source stream	main
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.

12.17 tIPsecIsaMemLowWatermark

Table 171: tIPsecIsaMemLowWatermark properties

Property name	Value
Application name	CHASSIS
Event ID	2150
Event name	tIPsecIsaMemLowWatermark
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.137
Default severity	minor
Source stream	main
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.

12.18 tIPsecIsaMemMax

Table 172: 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
Source stream	main
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.

Property name	Value
Effect	The system stops accepting new IKE states.
Recovery	Use fewer SAs for each IKE tunnel.

12.19 tmnxAlarmInputVoltageFailure

Table 173: 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
Source stream	main
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.

12.20 tmnxBluetoothModuleConnectionChg

Table 174: tmnxBluetoothModuleConnectionChg properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2187
Event name	tmnxBluetoothModuleConnectionChg
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.178
Default severity	minor
Source stream	main
Message format string	Bluetooth Module *$tmnxChassisNotifyCpmCardSlotNum$* got *$tmnx BluetoothModuleConnected$* to *$tmnxBluetoothModuleConnectedMac $*.
Cause	The tmnxBluetoothModuleConnectionChg notification is generated when a remote Bluetooth device connects with or disconnects from the indicated Bluetooth module.
Effect	A Bluetooth device has connected with or disconnected from a Bluetooth module.
Recovery	No recovery required.

12.21 tmnxCardResMacFdbHighUsgClr

Table 175: tmnxCardResMacFdbHighUsgClr properties

Property name	Value
Application name	CHASSIS
Event ID	5164
Event name	tmnxCardResMacFdbHighUsgClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.149
Default severity	minor
Source stream	main
Message format string	The FDB table usage for card *$tmnxMacScaleCardSlotNum$* is below 90% of the card limit
Cause	The tmnxCardResMacFdbHighUsgClr notification is generated when the FDB table size drops below 90% of the card limit.
Effect	The FDB table size for the card drops below 90% of the card limit.

Property name	Value
Recovery	None needed.

12.22 tmnxCardResMacFdbHighUsgSet

Table 176: tmnxCardResMacFdbHighUsgSet properties

Property name	Value
Application name	CHASSIS
Event ID	5163
Event name	tmnxCardResMacFdbHighUsgSet
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.148
Default severity	minor
Source stream	main
Message format string	The FDB table usage for card *$tmnxMacScaleCardSlotNum$* is above 95% of the card limit
Cause	The tmnxCardResMacFdbHighUsgSet notification is generated when the FDB table size exceeds 95% of the card limit.
Effect	The FDB table size for the card exceeds 95% of the card limit.
Recovery	None needed.

12.23 tmnxChassisAntiTheftModeBoot

Table 177: tmnxChassisAntiTheftModeBoot properties

Property name	Value
Application name	CHASSIS
Event ID	6014
Event name	tmnxChassisAntiTheftModeBoot
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.311

Property name	Value
Default severity	minor
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: system has booted in anti-theft mode
Cause	The tmnxChassisAntiTheftModeBoot notification is generated to indicate that the system has booted in Anti-Theft mode, and must be unlocked before protected features can be used.
Effect	N/A
Recovery	N/A

12.24 tmnxChassisAntiTheftUnlocked

Table 178: tmnxChassisAntiTheftUnlocked properties

Property name	Value
Application name	CHASSIS
Event ID	6015
Event name	tmnxChassisAntiTheftUnlocked
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.312
Default severity	minor
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: system in anti-theft mode has been unlocked
Cause	The tmnxChassisAntiTheftUnlocked notification is generated to indicate that the system has succesfully been unlocked following a reboot while Anti-Theft mode was enabled.
Effect	N/A
Recovery	N/A

12.25 tmnxChassisHiBwMcastAlarm

Table 179: 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
Source stream	main
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
Recovery	N/A

12.26 tmnxChassisNotificationClear

Table 180: 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
Source stream	main
Message format string	Clear *$tmnxHwClass$ $tmnxHwIndex$ $tmnxChassisNotifyOID$*

Property name	Value
Cause	A trap indicating the clear of a chassis notification identified by tmnx ChassisNotifyOID.
Effect	N/A
Recovery	N/A

12.27 tmnxChassisUpgradeComplete

Table 181: 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
Source stream	main
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 to the active CPM software version changed as part of the upgrade process.
Effect	N/A
Recovery	N/A

12.28 tmnxChassisUpgradeInProgress

Table 182: tmnxChassisUpgradeInProgress properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2033
Event name	tmnxChassisUpgradeInProgress
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.41
Default severity	major
Source stream	main
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 or XCMs 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	A software mismatch between the CPM and IOM or XCM is generally fine for a short duration (during an upgrade) but may not allow for correct long-term operation.
Recovery	Complete the upgrade of all IOMs or XCMs.

12.29 tmnxCpmALocalIcPortAvail

Table 183: tmnxCpmALocalIcPortAvail properties

Property name	Value
Application name	CHASSIS
Event ID	4009
Event name	tmnxCpmALocalIcPortAvail
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.6
Default severity	major
Source stream	main
Message format string	CPM *$tmnxChassisNotifyCpmCardSlotNum$* can reach the chassis using its local CPM interconnect ports

Property name	Value
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

12.30 tmnxCpmANoLocalIcPort

Table 184: 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
Source stream	main
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.

Property name	Value
Recovery	Ensure that all CPM interconnect ports in the system are properly cabled together with working cables.

12.31 tmnxCpmBLocalIcPortAvail

Table 185: 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
Source stream	main
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

12.32 tmnxCpmBNoLocalIcPort

Table 186: tmnxCpmBNoLocalIcPort properties

Property name	Value
Application name	CHASSIS
Event ID	4008

Property name	Value
Event name	tmnxCpmBNoLocalIcPort
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmIcPort Notifications.5
Default severity	major
Source stream	main
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.

12.33 tmnxCpmCardSyncFileNotPresent

Table 187: 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

Property name	Value
Source stream	main
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.
Effect	N/A
Recovery	N/A

12.34 tmnxCpmIcPortDDMClear

Table 188: 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
Source stream	main
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

12.35 tmnxCpmIcPortDDMFailure

Table 189: 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
Default severity	minor
Source stream	main
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

12.36 tmnxCpmIcPortDown

Table 190: 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
Source stream	main
Message format string	CPM interconnect port is not operational. Error code = *$tmnxCpmIcPort OperState$*

Property name	Value
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.

12.37 tmnxCpmIcPortSFFInserted

Table 191: 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
Source stream	main
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

12.38 tmnxCpmIcPortSFFRemoved

Table 192: 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
Source stream	main
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.
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.

12.39 tmnxCpmIcPortUp

Table 193: 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
Source stream	main
Message format string	CPM interconnect port is operational

Property name	Value
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

12.40 tmnxCpmMemSizeMismatch

Table 194: tmnxCpmMemSizeMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2153
Event name	tmnxCpmMemSizeMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.140
Default severity	major
Source stream	main
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.

12.41 tmnxCpmMemSizeMismatchClear

Table 195: 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
Source stream	main
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.

12.42 tmnxDcpCardFpEventOvrflw

Table 196: 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
Source stream	main
Message format string	TODO

Property name	Value
Cause	The tmnxDcpCardFpEventOvrflw notification is generated when a flood of distributed 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.

12.43 tmnxDcpCardFpEventOvrflwClr

Table 197: 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
Source stream	main
Message format string	TODO
Cause	The tmnxDcpCardFpEventOvrflwClr notification is generated when the event throttling has ended for distributed 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.

12.44 tmnxDcpCardSapEventOvrflw

Table 198: tmnxDcpCardSapEventOvrflw properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2085
Event name	tmnxDcpCardSapEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.73
Default severity	minor
Source stream	main
Message format string	TODO
Cause	The tmnxDcpCardSapEventOvrflw notification is generated when a flood of distributed 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.

12.45 tmnxDcpCardSapEventOvrflwClr

Table 199: 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
Source stream	main
Message format string	TODO
Cause	The tmnxDcpCardSapEventOvrflwClr notification is generated when the event throttling has ended for distributed 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.

12.46 tmnxDcpCardVrtrIfEventOvrflw

Table 200: 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
Source stream	main
Message format string	TODO
Cause	The tmnxDcpCardVrtrIfEventOvrflw notification is generated when a flood of distributed 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.

12.47 tmnxDcpCardVrtrIfEventOvrflwClr

Table 201: 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

Property name	Value
Source stream	main
Message format string	TODO
Cause	The tmnxDcpCardVrtrIfEventOvrflwClr notification is generated when the event throttling has ended for distributed CPU protection network-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.

12.48 tmnxDcpFpDynPoolUsageHiAlmClear

Table 202: 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
Source stream	main
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.

12.49 tmnxDcpFpDynPoolUsageHiAlmRaise

Table 203: tmnxDcpFpDynPoolUsageHiAlmRaise properties

Property name	Value
Application name	CHASSIS
Event ID	2087
Event name	tmnxDcpFpDynPoolUsageHiAlmRaise
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.75
Default severity	minor
Source stream	main
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.

12.50 tmnxEnvTempTooHigh

Table 204: 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
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: temperature too high

Property name	Value
Cause	Generated when the temperature sensor reading on an equipment object is greater than its configured threshold.
Effect	This could be causing intermittent errors and could also cause permanent damage to components.
Recovery	Remove or power down the affected cards, or improve the cooling to the node. More powerful fan trays may also be required.

12.51 tmnxEqBpEpromFail

Table 205: tmnxEqBpEpromFail properties

Property name	Value
Application name	CHASSIS
Event ID	2161
Event name	tmnxEqBpEpromFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.150
Default severity	critical
Source stream	main
Message format string	CPM BP EPROM could not be accessed
Cause	The tmnxEqBpEpromFail notification is generated when the active CPM is no longer able to access the backplane EPROM due to a hardware defect.
Effect	The active CPM is at risk of failing to initialize after node reboot due to not being able to access the BP EPROM to read the chassis type.
Recovery	Contact Nokia customer support.

12.52 tmnxEqBpEpromFailClear

Table 206: tmnxEqBpEpromFailClear properties

Property name	Value
Application name	CHASSIS
Event ID	2162
Event name	tmnxEqBpEpromFailClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.151
Default severity	cleared
Source stream	main
Message format string	CPM BP EPROM can now be accessed
Cause	The tmnxEqBpEpromFailClear notification is generated when the EPROM error condition is cleared.
Effect	N/A
Recovery	N/A

12.53 tmnxEqBpEpromWarning

Table 207: tmnxEqBpEpromWarning properties

Property name	Value
Application name	CHASSIS
Event ID	2163
Event name	tmnxEqBpEpromWarning
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.152
Default severity	minor
Source stream	main
Message format string	One CPM BP EPROM could not be accessed
Cause	The tmnxEqBpEpromWarning notification is generated when the active CPM is no longer able to access one backplane EPROM due to a hardware defect, but a redundant EPROM is present and accessible.
Effect	There is no effect on system operation.

Property name	Value
Recovery	No recovery action required.

12.54 tmnxEqBpEpromWarningClear

Table 208: tmnxEqBpEpromWarningClear properties

Property name	Value
Application name	CHASSIS
Event ID	2164
Event name	tmnxEqBpEpromWarningClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.153
Default severity	cleared
Source stream	main
Message format string	All CPM BP EPROMs can be accessed
Cause	The tmnxEqBpEpromWarningClear notification is generated when the backplane EPROM warning condition is cleared.
Effect	N/A
Recovery	N/A

12.55 tmnxEqCardChipIfCellEvent

Table 209: tmnxEqCardChipIfCellEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2103
Event name	tmnxEqCardChipIfCellEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.90

Property name	Value
Default severity	minor
Source stream	main
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.

12.56 tmnxEqCardChipIfDownEvent

Table 210: 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
Source stream	main
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	7750 SR/7450 ESS: The IOM or IMM will either remain operational or the card will reset along with its associated MDAs. 7950 XRS: The

Property name	Value
	associated XMA (MDA CLI context) will either remain operational or it will reset. The XCM (CLI card context) will not reset.
Recovery	Contact Nokia customer support.

12.57 tmnxEqCardFailure

Table 211: 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
Source stream	main
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 (or XCM), MDA (or XMA), SFM, CCM, CPM, Compact Flash, etc. The reason is indicated in the details of the log event or alarm, and also available in the tmnxChassisNotifyCardFailureReason attribute included in the SNMP notification.
Effect	The effect is dependent on the card that has failed. IOM (or XCM) or MDA (or XMA) failure will cause a loss of service for all services running on that card. A fabric failure can impact traffic to/from all cards. 7750 SR/7450 ESS - If the IOM/IMM fails then the two associated MDAs for the slot will also go down. 7950 XRS - If one out of two XMAs fails in a XCM slot then the XCM will remain up. If only one remaining operational XMA within a XCM slot fails, then the XCM will go into a booting operational state.
Recovery	Before taking any recovery steps, collect a tech-support file, then try resetting (clear) the card. If that doesn't work then try removing and then reinserting the card. If that doesn't work then replace the card.

12.58 tmnxEqCardFirmwareUpgraded

Table 212: 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
Source stream	main
Message format string	Class *$tmnxHwClass$* : firmware upgraded
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

12.59 tmnxEqCardInserted

Table 213: 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
Source stream	main
Message format string	Class *$tmnxHwClass$* : inserted

Property name	Value
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

12.60 tmnxEqCardMissing

Table 214: tmnxEqCardMissing properties

Property name	Value
Application name	CHASSIS
Event ID	6007
Event name	tmnxEqCardMissing
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.303
Default severity	major
Source stream	main
Message format string	Class *$tmnxHwClass$* : missing
Cause	The tmnxEqCardMissing notification is generated when the card configuration is present but the card is not detected in the slot.
Effect	The missing card will cause a loss of service for all services running on that card.
Recovery	Before taking any recovery steps collect a tech-support file, then try inserting a compatible card into the slot.

12.61 tmnxEqCardMissingClear

Table 215: tmnxEqCardMissingClear properties

Property name	Value
Application name	CHASSIS
Event ID	6008
Event name	tmnxEqCardMissingClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.304
Default severity	cleared
Source stream	main
Message format string	Class *$tmnxHwClass$* : missing clear
Cause	The tmnxEqCardMissingClear notification is generated when the card configuration is removed or the card is detected in the slot.
Effect	N/A
Recovery	N/A

12.62 tmnxEqCardPChipCamEvent

Table 216: tmnxEqCardPChipCamEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2076
Event name	tmnxEqCardPChipCamEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.64
Default severity	critical
Source stream	main
Message format string	A fault has been detected in the hardware on IOM *$tmnxSlotNum$*-forwarding engine *$tmnxCardComplexNumber$*
Cause	The tmnxEqCardPChipCamEvent notification is generated when either an IOM or a CPM experiences a persistent occurrence of a PChip CAM

Property name	Value
	error. On a CPM card, the tmnxCardComplexNumber will be fixed to the value zero (0).
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

12.63 tmnxEqCardPChipError

Table 217: 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
Source stream	main
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

12.64 tmnxEqCardPChipMemoryEvent

Table 218: 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
Source stream	main
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

12.65 tmnxEqCardQChipBufMemoryEvent

Table 219: 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
Source stream	main
Message format string	Possible messages:

Property name	Value
	• *$tmnxHwIndex$* experienced a Q-chip buffer memory error occurrence • Slot *$tmnxHwIndex$* experienced a Q-chip buffer memory error occurrence on complex *$tmnxCardComplexNumber$*
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.

12.66 tmnxEqCardQChipIntMemoryEvent

Table 220: 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
Source stream	main
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.

12.67 tmnxEqCardQChipStatsMemoryEvent

Table 221: tmnxEqCardQChipStatsMemoryEvent properties

Property name	Value
Application name	CHASSIS
Event ID	2099
Event name	tmnxEqCardQChipStatsMemoryEvent
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.87
Default severity	minor
Source stream	main
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.

12.68 tmnxEqCardRemoved

Table 222: tmnxEqCardRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	2003
Event name	tmnxEqCardRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.9

Property name	Value
Default severity	major
Source stream	main
Message format string	Class *$tmnxHwClass$* : removed
Cause	Generated when a card is removed from the chassis. The card type may be IOM (or XCM), MDA (or XMA), SFM, CCM, CPM, Compact Flash, etc.
Effect	The effect is dependent on the card that has been removed. IOM (or XCM) or MDA (or XMA) removal will cause a loss of service for all services running on that card. A fabric removal can impact traffic to/ from all cards.
Recovery	Before taking any recovery steps collect a tech-support file, then try reinserting the card. If that doesn't work then replace the card.

12.69 tmnxEqCardSoftResetAlarm

Table 223: 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
Source stream	main
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

12.70 tmnxEqCardTChipParityEvent

Table 224: 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
Source stream	main
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.

12.71 tmnxEqDataPathFailureProtImpact

Table 225: 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
Source stream	main

Property name	Value
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

12.72 tmnxEqEsaHostPortCrcAlarm

Table 226: tmnxEqEsaHostPortCrcAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	6009
Event name	tmnxEqEsaHostPortCrcAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.306
Default severity	minor
Source stream	main
Message format string	CRC errors in excess of the configured *$tmnxEsaHostPortNotifCrcAlrmValue$* threshold *$tmnxEsaHostPortNotifCrcMltiplier$**10e-*$tmnxEsaHostPortNotifCrcThreshold$* Set
Cause	The tmnxEqEsaHostPortCrcAlarm 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	tmnxEqEsaHostPortCrcAlarm is cleared by taking the port out of service (e.g. 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.

12.73 tmnxEqEsaHostPortCrcAlarmClear

Table 227: tmnxEqEsaHostPortCrcAlarmClear properties

Property name	Value
Application name	CHASSIS
Event ID	6010
Event name	tmnxEqEsaHostPortCrcAlarmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.307
Default severity	minor
Source stream	main
Message format string	CRC errors in excess of the configured *$tmnxEsaHostPortNotifCrcAlrmValue$* threshold *$tmnxEsaHostPortNotifCrcMltiplier$**10e-*$tmnxEsaHostPortNotifCrcThreshold$* Cleared
Cause	The tmnxEqEsaHostPortCrcAlarmClear is generated when an Ethernet port CRC alarm condition is cleared or disabled.
Effect	N/A
Recovery	N/A

12.74 tmnxEqFlashDataLoss

Table 228: 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
Source stream	main

Property name	Value
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

12.75 tmnxEqFlashDiskFull

Table 229: 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
Source stream	main
Message format string	Class *$tmnxHwClass$* : *$tmnxChassisNotifyDiskFullReason$*
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

12.76 tmnxEqFpgaSoftError

Table 230: tmnxEqFpgaSoftError properties

Property name	Value
Application name	CHASSIS
Event ID	2200
Event name	tmnxEqFpgaSoftError
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.211
Default severity	minor
Source stream	main
Message format string	Slot *$tmnxHwIndex$* detected an SEU event
Cause	The tmnxEqFpgaSoftError notification is for experimental use only and should remain suppressed unless advised otherwise by Nokia customer support.
Effect	Contact Nokia customer support.
Recovery	Contact Nokia customer support.

12.77 tmnxEqHwEnhancedCapability

Table 231: 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
Source stream	main
Message format string	CPM Upgrade In Progress. Card in slot *$tmnxCardSlotNum$* has enhanced capabilities.

Property name	Value
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).

12.78 tmnxEqHwEventDetected

Table 232: tmnxEqHwEventDetected properties

Property name	Value
Application name	CHASSIS
Event ID	2207
Event name	tmnxEqHwEventDetected
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.218
Default severity	minor
Source stream	main
Message format string	*$tmnxHwClass$ $tmnxChassisNotifyHwIndex$*: *$tmnxEqNotify HwEventType$* event detected. (detail: *$tmnxEqNotifyHwEventDetail$*, action:*$tmnxEqNotifyHwEventAction$*)
Cause	Generated when events or errors being monitored are detected by hardware component.
Effect	The system will perform the configured action on the hardware component.
Recovery	Check hardware component.

12.79 tmnxEqLowSwitchFabricCap

Table 233: 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
Source stream	main
Message format string	The switch fabric capacity is less than the forwarding capacity of *$tmnx HwClass$ $tmnxHwIndex$* 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.

12.80 tmnxEqLowSwitchFabricCapClear

Table 234: 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

Property name	Value
Source stream	main
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

12.81 tmnxEqMdaCfgNotCompatible

Table 235: tmnxEqMdaCfgNotCompatible properties

Property name	Value
Application name	CHASSIS
Event ID	2056
Event name	tmnxEqMdaCfgNotCompatible
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.44
Default severity	major
Source stream	main
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.

12.82 tmnxEqMdaIngrXplError

Table 236: 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
Source stream	main
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.

12.83 tmnxEqMdaSyncENotCompatible

Table 237: 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
Source stream	main
Message format string	Provisioned synchronous ethernet not compatible with equipped MDA

Property name	Value
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.

12.84 tmnxEqMdaXplError

Table 238: 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
Source stream	main
Message format string	MDA *$tmnxCardSlotNum$*/*$tmnxMDASlotNum$* experienced an egress XPL error occurrence.
Cause	The tmnxEqMdaXplError notification is generated when an MDA exhibits persistent egress XPL Errors.
Effect	N/A
Recovery	N/A

12.85 tmnxEqMgmtEthRedStandbyClear

Table 239: 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
Source stream	main
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.

12.86 tmnxEqMgmtEthRedStandbyRaise

Table 240: tmnxEqMgmtEthRedStandbyRaise properties

Property name	Value
Application name	CHASSIS
Event ID	2136
Event name	tmnxEqMgmtEthRedStandbyRaise
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.121
Default severity	minor
Source stream	main

Property name	Value
Message format string	The standby CPM's management Ethernet port *$tmnxChassisNotify MgmtEthRedPort$* 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.

12.87 tmnxEqOperStateChange

Table 241: tmnxEqOperStateChange properties

Property name	Value
Application name	CHASSIS
Event ID	2055
Event name	tmnxEqOperStateChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.85
Default severity	major
Source stream	main
Message format string	*$tmnxNotifyObjectName$* changed operational state: *$tmnxNotifyRow OperState$*
Cause	The tmnxEqOperStateChange notification is generated when a change occurred in the operational state on the piece of hardware.
Effect	If the state has changed to out of service, then all ports and services associated with the module change to out of service and traffic is impacted.
Recovery	Investigation is required to determine the cause of the change.

12.88 tmnxEqPhysChassisFanFailure

Table 242: 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
Source stream	main
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.

12.89 tmnxEqPhysChassisFanFailureClear

Table 243: 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
Source stream	main

Property name	Value
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.

12.90 tmnxEqPhysChassPowerSupAcFail

Table 244: 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
Source stream	main
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.

12.91 tmnxEqPhysChassPowerSupAcFailClr

Table 245: 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
Source stream	main
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.

12.92 tmnxEqPhysChassPowerSupDcFail

Table 246: 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
Source stream	main
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.

Property name	Value
Effect	The power supply is no longer operational.
Recovery	Insert a new power supply.

12.93 tmnxEqPhysChassPowerSupDcFailClr

Table 247: 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
Source stream	main
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.

12.94 tmnxEqPhysChassPowerSupInFail

Table 248: tmnxEqPhysChassPowerSupInFail properties

Property name	Value
Application name	CHASSIS
Event ID	2144
Event name	tmnxEqPhysChassPowerSupInFail

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.131
Default severity	critical
Source stream	main
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$* input failure
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.

12.95 tmnxEqPhysChassPowerSupInFailClr

Table 249: 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
Source stream	main
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.

12.96 tmnxEqPhysChassPowerSupOutFail

Table 250: tmnxEqPhysChassPowerSupOutFail properties

Property name	Value
Application name	CHASSIS
Event ID	2146
Event name	tmnxEqPhysChassPowerSupOutFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.133
Default severity	critical
Source stream	main
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.

12.97 tmnxEqPhysChassPowerSupOutFailCl

Table 251: 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
Source stream	main

Property name	Value
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.

12.98 tmnxEqPhysChassPowerSupOvrTmp

Table 252: tmnxEqPhysChassPowerSupOvrTmp properties

Property name	Value
Application name	CHASSIS
Event ID	2138
Event name	tmnxEqPhysChassPowerSupOvrTmp
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.125
Default severity	critical
Source stream	main
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.

12.99 tmnxEqPhysChassPowerSupOvrTmpClr

Table 253: 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
Source stream	main
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.

12.100 tmnxEqPowerCapacityExceeded

Table 254: 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
Source stream	main
Message format string	The system has reached maximum power capacity *$tmnxChassisNotify PowerCapacity$* watts

Property name	Value
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.

12.101 tmnxEqPowerCapacityExceededClear

Table 255: 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
Source stream	main
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.
Recovery	N/A

12.102 tmnxEqPowerLostCapacity

Table 256: 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
Source stream	main
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.

12.103 tmnxEqPowerLostCapacityClear

Table 257: 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
Source stream	main
Message format string	The system has reached a sustainable power capacity.

Property name	Value
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

12.104 tmnxEqPowerOverloadState

Table 258: 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
Source stream	main
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 cannot 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.

12.105 tmnxEqPowerOverloadStateClear

Table 259: tmnxEqPowerOverloadStateClear properties

Property name	Value
Application name	CHASSIS
Event ID	2097
Event name	tmnxEqPowerOverloadStateClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.85
Default severity	critical
Source stream	main
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

12.106 tmnxEqPowerSafetyAlertClear

Table 260: 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
Source stream	main
Message format string	Possible messages: • The system power capacity safety alert for zone *$tmnxChassisPwr MgmtZone$* has been disabled.

Property name	Value
	• 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

12.107 tmnxEqPowerSafetyAlertThreshold

Table 261: 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
Source stream	main
Message format string	The system power capacity for zone *$tmnxChassisPwrMgmtZone$* dropped below the configured safety alert threshold of *$tmnxChassisPwrMgmtSafetyAlert$* 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

12.108 tmnxEqPowerSafetyLevelClear

Table 262: 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
Source stream	main
Message format string	The peak nodal power for zone *$tmnxChassisPwrMgmtZone$* consumption dropped below the configured safety level threshold of *$tmnxChassisPwrMgmtSafetyLevel$* percent
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

12.109 tmnxEqPowerSafetyLevelThreshold

Table 263: 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
Source stream	main
Message format string	The peak nodal power for zone *$tmnxChassisPwrMgmtZone$* consumption exceeded the configured safety level threshold of *$tmnx ChassisPwrMgmtSafetyLevel$* percent

Property name	Value
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

12.110 tmnxEqPowerSupplyInserted

Table 264: 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
Source stream	main
Message format string	*$tmnxChassisNotifyHwIndex$* inserted
Cause	Generated when one of the chassis' power supplies is inserted.
Effect	N/A
Recovery	N/A

12.111 tmnxEqPowerSupplyRemoved

Table 265: tmnxEqPowerSupplyRemoved properties

Property name	Value
Application name	CHASSIS
Event ID	2011

Property name	Value
Event name	tmnxEqPowerSupplyRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.5
Default severity	major
Source stream	main
Message format string	*$tmnxChassisNotifyHwIndex$*, power lost
Cause	The tmnxEqPowerSupplyRemoved notification is generated when one of the power supplies is removed from the chassis or low input voltage is detected. The operating voltage range for the 7750 SR-7 and 7750 SR-12 is -40 to -72 VDC. The notification is generated if the system detects that the voltage of the power supply has dropped to -42.5 VDC.
Effect	Reduced power can cause intermittent errors and could also cause permanent damage to components.
Recovery	Reinsert the power supply or raise the input voltage above -42.5 VDC.

12.112 tmnxEqProvPowerCapacityAlm

Table 266: 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
Source stream	main
Message format string	The provisioned power capacity can no longer support configured devices.
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.

Property name	Value
Recovery	Increase the provisioned power capacity.

12.113 tmnxEqProvPowerCapacityAlmClr

Table 267: 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
Source stream	main
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

12.114 tmnxEqSyncIfTimingBITS2Alarm

Table 268: 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
Source stream	main
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

12.115 tmnxEqSyncIfTimingBITS2AlarmClr

Table 269: 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
Source stream	main
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

12.116 tmnxEqSyncIfTimingBITS2Quality

Table 270: 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
Source stream	main
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

12.117 tmnxEqSyncIfTimingBITSAlarm

Table 271: 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
Source stream	main

Property name	Value
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

12.118 tmnxEqSyncIfTimingBITSAlarmClear

Table 272: 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
Source stream	main
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

12.119 tmnxEqSyncIfTimingBITSOutRefChg

Table 273: 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
Source stream	main
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
Recovery	N/A

12.120 tmnxEqSyncIfTimingBITSQuality

Table 274: 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
Source stream	main
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

Property name	Value
Recovery	N/A

12.121 tmnxEqSyncIfTimingGnss2Alarm

Table 275: tmnxEqSyncIfTimingGnss2Alarm properties

Property name	Value
Application name	CHASSIS
Event ID	2227
Event name	tmnxEqSyncIfTimingGnss2Alarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.238
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on GNSS2 reference
Cause	Generated when an alarm condition on the gnss2 timing reference is detected. The type of alarm (los, oof, etc) is indicated in the details of the log event or alarm, and is also available in the tmnxSyncIfTiming NotifyAlarm attribute included in the SNMP notification. The SNMP notification will have the same indices as those of the tmnxCpmCard Table.
Effect	Timing reference gnss2 cannot be used as a source of timing into the central clock.
Recovery	Address issues with the signal associated with timing reference gnss2.

12.122 tmnxEqSyncIfTimingGnss2AlarmClr

Table 276: tmnxEqSyncIfTimingGnss2AlarmClr properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2229
Event name	tmnxEqSyncIfTimingGnss2AlarmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.240
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on GNSS2 reference cleared
Cause	Generated when an alarm condition on the gnss2 timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

12.123 tmnxEqSyncIfTimingGnss2Quality

Table 277: tmnxEqSyncIfTimingGnss2Quality properties

Property name	Value
Application name	CHASSIS
Event ID	2225
Event name	tmnxEqSyncIfTimingGnss2Quality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.236
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, reference GNSS2 received quality level *$tmnxSyncIfTimingGnss2RxQltyLevel$*
Cause	Generated when there is a change of the received quality level on timing reference gnss2.
Effect	N/A
Recovery	N/A

12.124 tmnxEqSyncIfTimingGnssAlarm

Table 278: tmnxEqSyncIfTimingGnssAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2226
Event name	tmnxEqSyncIfTimingGnssAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.237
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on GNSS reference
Cause	Generated when an alarm condition on the gnss timing reference is detected. The type of alarm (los, oof, etc) is indicated in the details of the log event or alarm, and is also available in the tmnxSyncIfTiming NotifyAlarm attribute included in the SNMP notification. The SNMP notification will have the same indices as those of the tmnxCpmCard Table.
Effect	Timing reference gnss cannot be used as a source of timing into the central clock.
Recovery	Address issues with the signal associated with timing reference gnss.

12.125 tmnxEqSyncIfTimingGnssAlarmClr

Table 279: tmnxEqSyncIfTimingGnssAlarmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2228
Event name	tmnxEqSyncIfTimingGnssAlarmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.239

Property name	Value
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on GNSS reference cleared
Cause	Generated when an alarm condition on the gnss timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

12.126 tmnxEqSyncIfTimingGnssQuality

Table 280: tmnxEqSyncIfTimingGnssQuality properties

Property name	Value
Application name	CHASSIS
Event ID	2224
Event name	tmnxEqSyncIfTimingGnssQuality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.235
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, reference GNSS received quality level *$tmnxSyncIfTimingGnssRxQltyLevel$*
Cause	Generated when there is a change of the received quality level on timing reference gnss.
Effect	N/A
Recovery	N/A

12.127 tmnxEqSyncIfTimingHoldover

Table 281: 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
Source stream	main
Message format string	Synchronous Timing interface in holdover state
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	Any node-timed ports will have very slow frequency drift limited by the central clock oscillator stability. The oscillator meets the holdover requirements of a Stratum 3 and G.813 Option 1 clock.
Recovery	Address issues with the central clock input references.

12.128 tmnxEqSyncIfTimingHoldoverClear

Table 282: 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
Source stream	main
Message format string	Synchronous Timing interface holdover state cleared

Property name	Value
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

12.129 tmnxEqSyncIfTimingPTPAlarm

Table 283: tmnxEqSyncIfTimingPTPAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2080
Event name	tmnxEqSyncIfTimingPTPAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.68
Default severity	minor
Source stream	main
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

12.130 tmnxEqSyncIfTimingPTPAlarmClr

Table 284: 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
Source stream	main
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

12.131 tmnxEqSyncIfTimingPTPQuality

Table 285: tmnxEqSyncIfTimingPTPQuality properties

Property name	Value
Application name	CHASSIS
Event ID	2079
Event name	tmnxEqSyncIfTimingPTPQuality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.67
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, reference PTP received quality level *$tmnxSyncIfTimingPTPRxQltyLevel$*

Property name	Value
Cause	Generated when there is a change of the received quality level on the Precision Timing Protocol (PTP).
Effect	N/A
Recovery	N/A

12.132 tmnxEqSyncIfTimingRef1Alarm

Table 286: 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
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on reference 1
Cause	Generated when an alarm condition on the first timing reference is detected. The type of alarm (los, oof, etc) is indicated in the details of the log event or alarm, and is also available in the tmnxSyncIfTiming NotifyAlarm attribute included in the SNMP notification. The SNMP notification will have the same indices as those of the tmnxCpmCard Table.
Effect	Indicated timing reference (1, 2, or BITS) cannot be used as a source of timing into the central clock.
Recovery	Address issues with the signal associated with indicated timing reference (1, 2, or BITS).

12.133 tmnxEqSyncIfTimingRef1AlarmClear

Table 287: 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
Source stream	main
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

12.134 tmnxEqSyncIfTimingRef1Quality

Table 288: 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
Source stream	main
Message format string	Synchronous Timing interface, reference 1 received quality level *$tmnxSyncIfTimingRef1RxQltyLevel$*

Property name	Value
Cause	Generated when there is a change of the received quality level on timing reference 1.
Effect	N/A
Recovery	N/A

12.135 tmnxEqSyncIfTimingRef2Alarm

Table 289: 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
Source stream	main
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

12.136 tmnxEqSyncIfTimingRef2AlarmClear

Table 290: tmnxEqSyncIfTimingRef2AlarmClear properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2022
Event name	tmnxEqSyncIfTimingRef2AlarmClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.31
Default severity	minor
Source stream	main
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.
Effect	N/A
Recovery	N/A

12.137 tmnxEqSyncIfTimingRef2Quality

Table 291: 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
Source stream	main
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

12.138 tmnxEqSyncIfTimingRefSwitch

Table 292: 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
Source stream	main
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

12.139 tmnxEqSyncIfTimingSyncE2Alarm

Table 293: tmnxEqSyncIfTimingSyncE2Alarm properties

Property name	Value
Application name	CHASSIS
Event ID	2205
Event name	tmnxEqSyncIfTimingSyncE2Alarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.216
Default severity	minor
Source stream	main

Property name	Value
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on SYNCE2 reference
Cause	Generated when an alarm condition on the SYNCE 2 timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

12.140 tmnxEqSyncIfTimingSyncE2AlarmClr

Table 294: tmnxEqSyncIfTimingSyncE2AlarmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2206
Event name	tmnxEqSyncIfTimingSyncE2AlarmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.217
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on SYNCE2 reference cleared
Cause	Generated when an alarm condition on the SYNCE 2 timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

12.141 tmnxEqSyncIfTimingSyncE2Quality

Table 295: tmnxEqSyncIfTimingSyncE2Quality properties

Property name	Value
Application name	CHASSIS
Event ID	2202
Event name	tmnxEqSyncIfTimingSyncE2Quality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.213
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, reference SYNCE2 received quality level *$tmnxSyncIfTimingSyncE2RxQltyLevl$*
Cause	Generated when there is a change of the received quality level on timing reference synce2.
Effect	N/A
Recovery	N/A

12.142 tmnxEqSyncIfTimingSyncEAlarm

Table 296: tmnxEqSyncIfTimingSyncEAlarm properties

Property name	Value
Application name	CHASSIS
Event ID	2203
Event name	tmnxEqSyncIfTimingSyncEAlarm
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.214
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on SYNCE reference

Property name	Value
Cause	Generated when an alarm condition on the SYNCE timing reference is detected. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

12.143 tmnxEqSyncIfTimingSyncEAlarmClr

Table 297: tmnxEqSyncIfTimingSyncEAlarmClr properties

Property name	Value
Application name	CHASSIS
Event ID	2204
Event name	tmnxEqSyncIfTimingSyncEAlarmClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.215
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, alarm *$tmnxSyncIfTimingNotifyAlarm$* on SYNCE reference cleared
Cause	Generated when an alarm condition on the SYNCE timing reference is cleared. This notification will have the same indices as those of the tmnxCpmCardTable.
Effect	N/A
Recovery	N/A

12.144 tmnxEqSyncIfTimingSyncEQuality

Table 298: tmnxEqSyncIfTimingSyncEQuality properties

Property name	Value
Application name	CHASSIS
Event ID	2201
Event name	tmnxEqSyncIfTimingSyncEQuality
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.212
Default severity	minor
Source stream	main
Message format string	Synchronous Timing interface, reference SYNCE received quality level *$tmnxSyncIfTimingSyncERxQltyLevel$*
Cause	Generated when there is a change of the received quality level on timing reference synce.
Effect	N/A
Recovery	N/A

12.145 tmnxEqSyncIfTimingSystemQuality

Table 299: 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
Source stream	main
Message format string	Synchronous Timing interface, System Quality Level changed to *$tmnx SyncIfTimingSystemQltyLevel$*
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

Property name	Value
	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.

12.146 tmnxEqWrongCard

Table 300: 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
Source stream	main
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 (or XCM), Fabric, MDA (or XMA), MCM, CPM module, etc.
Effect	The effect is dependent on the card that has been incorrectly inserted. Incorrect IOM (or XCM) or MDA (or XMA) insertion will cause a loss of service for all services running on that card.

Property name	Value
Recovery	Insert the correct card into the correct slot, and ensure the slot is configured for the correct type of card.

12.147 tmnxEsaCleared

Table 301: tmnxEsaCleared properties

Property name	Value
Application name	CHASSIS
Event ID	2213
Event name	tmnxEsaCleared
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.224
Default severity	major
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* cleared
Cause	The tmnxEsaCleared notification is generated when an ESA is cleared or rebooted.
Effect	N/A
Recovery	N/A

12.148 tmnxEsaConnected

Table 302: tmnxEsaConnected properties

Property name	Value
Application name	CHASSIS
Event ID	2210
Event name	tmnxEsaConnected
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.221

Property name	Value
Default severity	minor
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* connected
Cause	The tmnxEsaConnected notification is generated when a new ESA is connected.
Effect	N/A
Recovery	N/A

12.149 tmnxEsaDisconnected

Table 303: tmnxEsaDisconnected properties

Property name	Value
Application name	CHASSIS
Event ID	2211
Event name	tmnxEsaDisconnected
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.222
Default severity	major
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* disconnected
Cause	The tmnxEsaDisconnected notification is generated when an ESA is disconnected.
Effect	N/A
Recovery	N/A

12.150 tmnxEsaDiscovered

Table 304: tmnxEsaDiscovered properties

Property name	Value
Application name	CHASSIS
Event ID	2209
Event name	tmnxEsaDiscovered
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.220
Default severity	minor
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* discovered
Cause	The tmnxEsaDiscovered notification is generated when a new ESA is discovered by the system.
Effect	N/A
Recovery	N/A

12.151 tmnxEsaFailure

Table 305: tmnxEsaFailure properties

Property name	Value
Application name	CHASSIS
Event ID	2212
Event name	tmnxEsaFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.223
Default severity	major
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* failed with reason *$tmnxEsaStatsOperFlags$*
Cause	The tmnxEsaFailure notification is generated when a failure occurs on an ESA.
Effect	N/A

Property name	Value
Recovery	N/A

12.152 tmnxEsaFirmwareUpgradeDone

Table 306: tmnxEsaFirmwareUpgradeDone properties

Property name	Value
Application name	CHASSIS
Event ID	6012
Event name	tmnxEsaFirmwareUpgradeDone
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.309
Default severity	minor
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* Firmware upgrade done - *$firmwareUpgrade Stage$*
Cause	The tmnxEsaFirmwareUpgradeInProgress notification is generated to indicate whenever a certain upgrade stage/device is complete.
Effect	N/A
Recovery	N/A

12.153 tmnxEsaFirmwareUpgradeFailed

Table 307: tmnxEsaFirmwareUpgradeFailed properties

Property name	Value
Application name	CHASSIS
Event ID	6013
Event name	tmnxEsaFirmwareUpgradeFailed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.310

Property name	Value
Default severity	minor
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* Firmware upgrade failed - *$firmwareUpgrade Stage$*
Cause	The tmnxEsaFirmwareUpgradeFailed notification is generated to indicate that the ESA firmware upgrade did not successfully finish. The ESA has one or more devices that still require firmware upgrade.
Effect	An ESA running with partially upgraded firmware might potentially exhibit sub-optimal performance, or other service affecting issues.
Recovery	A manual clear of the esa using the clear esa command, or power cycling the ESA would trigger a firmware upgrade to be re-attempted.

12.154 tmnxEsaFirmwareUpgradeInProgress

Table 308: tmnxEsaFirmwareUpgradeInProgress properties

Property name	Value
Application name	CHASSIS
Event ID	6011
Event name	tmnxEsaFirmwareUpgradeInProgress
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.308
Default severity	minor
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* Firmware upgrade in progress - *$firmware UpgradeStage$*
Cause	The tmnxEsaFirmwareUpgradeInProgress notification is generated to indicate the different upgrade stages/devices and the expected ESA reboots.
Effect	N/A
Recovery	N/A

12.155 tmnxEsaFirmwareUpgradeStarted

Table 309: tmnxEsaFirmwareUpgradeStarted properties

Property name	Value
Application name	CHASSIS
Event ID	2230
Event name	tmnxEsaFirmwareUpgradeStarted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.241
Default severity	minor
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* Firmware upgrade started
Cause	The tmnxEsaFirmwareUpgradeStarted notification is generated when an ESA requests a firmware upgrade and is in progress.
Effect	N/A
Recovery	N/A

12.156 tmnxEsaHwFanBankFailRedun

Table 310: tmnxEsaHwFanBankFailRedun properties

Property name	Value
Application name	CHASSIS
Event ID	2414
Event name	tmnxEsaHwFanBankFailRedun
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.279
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan bank status failed-redundant

Property name	Value
Cause	The tmnxEsaHwFanBankFailRedun notification is generated when one or more ESA fans fail, compromising the fan bank redundancy.
Effect	ESA cooling may be inadequate if fan failure occurs.
Recovery	Contact Nokia customer support.

12.157 tmnxEsaHwFanBankFailRedunClr

Table 311: tmnxEsaHwFanBankFailRedunClr properties

Property name	Value
Application name	CHASSIS
Event ID	2415
Event name	tmnxEsaHwFanBankFailRedunClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.280
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan bank failed-redundant status cleared, now *$tmnxEsaStatsFanRedundancy$*
Cause	The tmnxEsaHwFanBankFailRedunClr notification is generated when all ESA fans recover, restoring the fan bank redundancy.
Effect	N/A
Recovery	N/A

12.158 tmnxEsaHwFanBankNonRedun

Table 312: tmnxEsaHwFanBankNonRedun properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2412
Event name	tmnxEsaHwFanBankNonRedun
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.277
Default severity	major
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan bank status non-redundant
Cause	The tmnxEsaHwFanBankNonRedun notification is generated when a condition compromises the ESA fan bank redundancy.
Effect	ESA cooling may be inadequate if fan failure occurs.
Recovery	Contact Nokia customer support.

12.159 tmnxEsaHwFanBankNonRedunClr

Table 313: tmnxEsaHwFanBankNonRedunClr properties

Property name	Value
Application name	CHASSIS
Event ID	2413
Event name	tmnxEsaHwFanBankNonRedunClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.278
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan bank non-redundant status cleared, now *$tmnxEsaStatsFanRedundancy$*
Cause	The tmnxEsaHwFanBankNonRedunClr notification is generated when the ESA fan bank redundancy is restored.
Effect	N/A
Recovery	N/A

12.160 tmnxEsaHwFanStatusDegraded

Table 314: tmnxEsaHwFanStatusDegraded properties

Property name	Value
Application name	CHASSIS
Event ID	2416
Event name	tmnxEsaHwFanStatusDegraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.281
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan status degraded
Cause	The tmnxEsaHwFanStatusDegraded notification is generated when one or more ESA fans are degraded.
Effect	ESA cooling may be inadequate.
Recovery	Contact Nokia customer support.

12.161 tmnxEsaHwFanStatusDegradedClr

Table 315: tmnxEsaHwFanStatusDegradedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2417
Event name	tmnxEsaHwFanStatusDegradedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.282
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan degraded status cleared, now *$tmnxEsaStatsFanStatus$*

Property name	Value
Cause	The tmnxEsaHwFanStatusDegradedClr notification is generated when ESA fans are no longer degraded.
Effect	N/A
Recovery	N/A

12.162 tmnxEsaHwFanStatusFailed

Table 316: tmnxEsaHwFanStatusFailed properties

Property name	Value
Application name	CHASSIS
Event ID	2418
Event name	tmnxEsaHwFanStatusFailed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.283
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan status failed
Cause	The tmnxEsaHwFanStatusFailed notification is generated when one or more ESA fans fail.
Effect	ESA cooling may be inadequate.
Recovery	Contact Nokia customer support.

12.163 tmnxEsaHwFanStatusFailedClr

Table 317: tmnxEsaHwFanStatusFailedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2419

Property name	Value
Event name	tmnxEsaHwFanStatusFailedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.284
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* fan failed status cleared, now *$tmnxEsaStatsFanStatus$*
Cause	The tmnxEsaHwFanStatusFailedClr notification is generated when the ESA fans are restored.
Effect	N/A
Recovery	N/A

12.164 tmnxEsaHwPwrSup1Degraded

Table 318: tmnxEsaHwPwrSup1Degraded properties

Property name	Value
Application name	CHASSIS
Event ID	2404
Event name	tmnxEsaHwPwrSup1Degraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.269
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 1 status degraded
Cause	The tmnxEsaHwPwrSup1Degraded notification is generated when the ESA power supply 1 is degraded.
Effect	Power supply operation and reliability may be affected.
Recovery	Contact Nokia customer support.

12.165 tmnxEsaHwPwrSup1DegradedClr

Table 319: tmnxEsaHwPwrSup1DegradedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2405
Event name	tmnxEsaHwPwrSup1DegradedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.270
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 1 degraded status cleared, now *$tmnxEsaStatsPowerSupply1Status$*
Cause	The tmnxEsaHwPwrSup1DegradedClr notification is generated when the ESA power supply 1 is no longer degraded.
Effect	N/A
Recovery	N/A

12.166 tmnxEsaHwPwrSup1Failed

Table 320: tmnxEsaHwPwrSup1Failed properties

Property name	Value
Application name	CHASSIS
Event ID	2406
Event name	tmnxEsaHwPwrSup1Failed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.271
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 1 status failed

Property name	Value
Cause	The tmnxEsaHwPwrSup1Failed notification is generated when the ESA power supply 1 fails.
Effect	Power supply and redundancy are affected. ESA operation may be affected.
Recovery	Contact Nokia customer support.

12.167 tmnxEsaHwPwrSup1FailedClr

Table 321: tmnxEsaHwPwrSup1FailedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2407
Event name	tmnxEsaHwPwrSup1FailedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.272
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 1 failed status cleared, now *$tmnxEsaStatsPowerSupply1Status$*
Cause	The tmnxEsaHwPwrSup1FailedClr notification is generated when the ESA power supply 1 is restored.
Effect	N/A
Recovery	N/A

12.168 tmnxEsaHwPwrSup2Degraded

Table 322: tmnxEsaHwPwrSup2Degraded properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2408
Event name	tmnxEsaHwPwrSup2Degraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.273
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 2 status degraded
Cause	The tmnxEsaHwPwrSup2Degraded notification is generated when the ESA power supply 2 is degraded.
Effect	Power supply operation and reliability may be affected.
Recovery	Contact Nokia customer support.

12.169 tmnxEsaHwPwrSup2DegradedClr

Table 323: tmnxEsaHwPwrSup2DegradedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2409
Event name	tmnxEsaHwPwrSup2DegradedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.274
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 2 degraded status cleared, now *$tmnxEsaStatsPowerSupply2Status$*
Cause	The tmnxEsaHwPwrSup2DegradedClr notification is generated when the ESA power supply 2 is no longer degraded.
Effect	N/A
Recovery	N/A

12.170 tmnxEsaHwPwrSup2Failed

Table 324: tmnxEsaHwPwrSup2Failed properties

Property name	Value
Application name	CHASSIS
Event ID	2410
Event name	tmnxEsaHwPwrSup2Failed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.275
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply 2 status failed
Cause	The tmnxEsaHwPwrSup2Failed notification is generated when the ESA power supply 2 fails.
Effect	Power supply and redundancy are affected. ESA operation may be affected.
Recovery	Contact Nokia customer support.

12.171 tmnxEsaHwPwrSup2FailedClr

Table 325: tmnxEsaHwPwrSup2FailedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2411
Event name	tmnxEsaHwPwrSup2FailedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.276
Default severity	cleared
Source stream	main

Property name	Value
Message format string	ESA *$tmnxHwClass$* power supply 2 failed status cleared, now *$tmnxEsaStatsPowerSupply2Status$*
Cause	The tmnxEsaHwPwrSup2FailedClr notification is generated when the ESA power supply 2 is restored.
Effect	N/A
Recovery	N/A

12.172 tmnxEsaHwPwrSupBankFailRedun

Table 326: tmnxEsaHwPwrSupBankFailRedun properties

Property name	Value
Application name	CHASSIS
Event ID	2424
Event name	tmnxEsaHwPwrSupBankFailRedun
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.289
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply bank status failed-redundant
Cause	The tmnxEsaHwPwrSupBankFailRedun notification is generated when the ESA power supply redundancy fails.
Effect	ESA operation may be affected if additional power supply failures occur.
Recovery	Contact Nokia customer support.

12.173 tmnxEsaHwPwrSupBankFailRedunClr

Table 327: tmnxEsaHwPwrSupBankFailRedunClr properties

Property name	Value
Application name	CHASSIS
Event ID	2425
Event name	tmnxEsaHwPwrSupBankFailRedunClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.290
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply bank failed-redundant status cleared, now *$tmnxEsaStatsPwrSupRedundancy$*
Cause	The tmnxEsaHwPwrSupBankFailRedunClr notification is generated when the ESA power supplies regain redundancy.
Effect	N/A
Recovery	N/A

12.174 tmnxEsaHwPwrSupBankNonRedun

Table 328: tmnxEsaHwPwrSupBankNonRedun properties

Property name	Value
Application name	CHASSIS
Event ID	2422
Event name	tmnxEsaHwPwrSupBankNonRedun
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.287
Default severity	major
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply bank status non-redundant
Cause	The tmnxEsaHwPwrSupBankNonRedun notification is generated when the ESA power supply redundancy is degraded.
Effect	ESA may lose power supply redundancy if power supply failures occur.

Property name	Value
Recovery	Contact Nokia customer support.

12.175 tmnxEsaHwPwrSupBankNonRedunClr

Table 329: tmnxEsaHwPwrSupBankNonRedunClr properties

Property name	Value
Application name	CHASSIS
Event ID	2423
Event name	tmnxEsaHwPwrSupBankNonRedunClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.288
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply bank non-redundant status cleared, now *$tmnxEsaStatsPwrSupRedundancy$*
Cause	The tmnxEsaHwPwrSupBankNonRedunClr notification is generated when the ESA power supplies return to a fully redundant state.
Effect	N/A
Recovery	N/A

12.176 tmnxEsaHwPwrSupMismatch

Table 330: tmnxEsaHwPwrSupMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2420
Event name	tmnxEsaHwPwrSupMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.285

Property name	Value
Default severity	major
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply mismatch
Cause	The tmnxEsaHwPwrSupMismatch notification is generated when the ESA power supplies do not match.
Effect	ESA power supplies must be matched.
Recovery	Equip the ESA with matching power supplies.

12.177 tmnxEsaHwPwrSupMismatchClr

Table 331: tmnxEsaHwPwrSupMismatchClr properties

Property name	Value
Application name	CHASSIS
Event ID	2421
Event name	tmnxEsaHwPwrSupMismatchClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.286
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* power supply mismatch - cleared, now *$tmnxEsaStatsPwrSupMismatchStatus$*
Cause	The tmnxEsaHwPwrSupMismatchClr notification is generated when the ESA power supplies are no longer mismatched.
Effect	N/A
Recovery	N/A

12.178 tmnxEsaHwStatusCritical

Table 332: tmnxEsaHwStatusCritical properties

Property name	Value
Application name	CHASSIS
Event ID	2402
Event name	tmnxEsaHwStatusCritical
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.267
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* aggregate hardware status critical
Cause	The tmnxEsaHwStatusCritical notification is generated when the ESA hardware status is critical.
Effect	Service may be affected.
Recovery	Contact Nokia customer support.

12.179 tmnxEsaHwStatusCriticalClr

Table 333: tmnxEsaHwStatusCriticalClr properties

Property name	Value
Application name	CHASSIS
Event ID	2403
Event name	tmnxEsaHwStatusCriticalClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.268
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* aggregate hardware status critical - cleared, now *$tmnxEsaStatsHardwareStatus$*
Cause	The tmnxEsaHwStatusCriticalClr notification is generated when the ESA hardware status is no longer critical.
Effect	N/A

Property name	Value
Recovery	N/A

12.180 tmnxEsaHwStatusDegraded

Table 334: tmnxEsaHwStatusDegraded properties

Property name	Value
Application name	CHASSIS
Event ID	2400
Event name	tmnxEsaHwStatusDegraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.265
Default severity	major
Source stream	main
Message format string	ESA *$tmnxHwClass$* aggregate hardware status degraded
Cause	The tmnxEsaHwStatusDegraded notification is generated when one or more ESA hardware components are degraded.
Effect	Service may be affected.
Recovery	Contact Nokia customer support.

12.181 tmnxEsaHwStatusDegradedClr

Table 335: tmnxEsaHwStatusDegradedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2401
Event name	tmnxEsaHwStatusDegradedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.266

Property name	Value
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* aggregate hardware degraded status cleared, now *$tmnxEsaStatsHardwareStatus$*
Cause	The tmnxEsaHwStatusDegradedClr notification is generated when ESA hardware components are no longer degraded.
Effect	N/A
Recovery	N/A

12.182 tmnxEsaHwTemperatureDegraded

Table 336: tmnxEsaHwTemperatureDegraded properties

Property name	Value
Application name	CHASSIS
Event ID	2426
Event name	tmnxEsaHwTemperatureDegraded
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.291
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* temperature status degraded
Cause	The tmnxEsaHwTemperatureDegraded notification is generated when the ESA temperature is outside the expected operating range.
Effect	If the ESA temperature remains outside the expected operating range, the ESA may shut down.
Recovery	The ESA may need manual maintenance to rectify the issue. Contact Nokia customer support.

12.183 tmnxEsaHwTemperatureDegradedClr

Table 337: tmnxEsaHwTemperatureDegradedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2427
Event name	tmnxEsaHwTemperatureDegradedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.292
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* temperature degraded status cleared, now *$tmnxEsaStatsTemperatureStatus$*
Cause	The tmnxEsaHwTemperatureDegradedClr notification is generated when the ESA returns to a temperature within the expected operating range.
Effect	N/A
Recovery	N/A

12.184 tmnxEsaHwTemperatureFailed

Table 338: tmnxEsaHwTemperatureFailed properties

Property name	Value
Application name	CHASSIS
Event ID	2428
Event name	tmnxEsaHwTemperatureFailed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.293
Default severity	critical
Source stream	main
Message format string	ESA *$tmnxHwClass$* temperature status failed
Cause	The tmnxEsaHwTemperatureFailed notification is generated when the ESA temperature is critical.

Property name	Value
Effect	If the ESA temperature remains outside the expected operating range, the ESA may shut down.
Recovery	The ESA may need manual maintenance to rectify the issue. Contact Nokia customer support.

12.185 tmnxEsaHwTemperatureFailedClr

Table 339: tmnxEsaHwTemperatureFailedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2429
Event name	tmnxEsaHwTemperatureFailedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.294
Default severity	cleared
Source stream	main
Message format string	ESA *$tmnxHwClass$* temperature failed status cleared, now *$tmnxEsaStatsTemperatureStatus$*
Cause	The tmnxEsaHwTemperatureFailedClr notification is generated when the ESA returns to a temperature within the expected operating range.
Effect	N/A
Recovery	N/A

12.186 tmnxEsaStolenTimeDetected

Table 340: tmnxEsaStolenTimeDetected properties

Property name	Value
Application name	CHASSIS
Event ID	2399

Property name	Value
Event name	tmnxEsaStolenTimeDetected
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.305
Default severity	major
Source stream	main
Message format string	ESA *$tmnxEsaNotifyId$* detected *$stolenTimeEvent$*
Cause	The tmnxEsaStolenTimeDetected notification is generated when stolen time monitoring on the ESA detects periods of time that ESA-VMs are ready to run, but are unable to do so. The stolen time is reported in ms.
Effect	If the periods of stolen time exceeds a certain value, they may result in ESA-VM reset or temporary loss of connection of the ESA with the host node.
Recovery	Before taking any recovery steps, collect a tech-support and consult with support for best recovery method.

12.187 tmnxEsaVmBooted

Table 341: tmnxEsaVmBooted properties

Property name	Value
Application name	CHASSIS
Event ID	2215
Event name	tmnxEsaVmBooted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.226
Default severity	major
Source stream	main
Message format string	ESA-VM *$tmnxEsaNotifyId$*/ *$tmnxEsaVmNotifyId$* booted
Cause	The tmnxEsaVmBooted notification is generated when an ESA VM is booted.
Effect	N/A
Recovery	N/A

12.188 tmnxEsaVmCleared

Table 342: tmnxEsaVmCleared properties

Property name	Value
Application name	CHASSIS
Event ID	2217
Event name	tmnxEsaVmCleared
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.228
Default severity	minor
Source stream	main
Message format string	ESA-VM *$tmnxEsaNotifyId$*/*$tmnxEsaVmNotifyId$* reset
Cause	The tmnxEsaVmCleared notification is generated when an ESA VM is cleared or restarted.
Effect	N/A
Recovery	N/A

12.189 tmnxEsaVmCreated

Table 343: tmnxEsaVmCreated properties

Property name	Value
Application name	CHASSIS
Event ID	2214
Event name	tmnxEsaVmCreated
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.225
Default severity	major
Source stream	main
Message format string	ESA-VM *$tmnxEsaNotifyId$*/*$tmnxEsaVmNotifyId$* created

Property name	Value
Cause	The tmnxEsaVmCreated notification is generated when an ESA VM is created.
Effect	N/A
Recovery	N/A

12.190 tmnxEsaVmFailure

Table 344: tmnxEsaVmFailure properties

Property name	Value
Application name	CHASSIS
Event ID	2218
Event name	tmnxEsaVmFailure
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.229
Default severity	major
Source stream	main
Message format string	ESA-VM *$tmnxEsaNotifyId$*/*$tmnxEsaVmNotifyId$* failed with reason *$tmnxEsaVmStatsOperFlags$*
Cause	The tmnxEsaVmFailure notification is generated when an ESA VM crashes.
Effect	N/A
Recovery	N/A

12.191 tmnxEsaVmRemoved

Table 345: tmnxEsaVmRemoved properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2216
Event name	tmnxEsaVmRemoved
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.227
Default severity	major
Source stream	main
Message format string	ESA-VM *$tmnxEsaNotifyId$*/*$tmnxEsaVmNotifyId$* destroyed
Cause	The tmnxEsaVmRemoved notification is generated when an ESA VM is removed.
Effect	N/A
Recovery	N/A

12.192 tmnxExtStandbyCpmReboot

Table 346: 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
Source stream	main
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 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.

Property name	Value
Effect	The extension standby CPM will reboot.
Recovery	There is no recovery for this notification.

12.193 tmnxExtStandbyCpmRebootFail

Table 347: 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
Source stream	main
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.

12.194 tmnxFPResourcePolicyModified

Table 348: tmnxFPResourcePolicyModified properties

Property name	Value
Application name	CHASSIS
Event ID	2222
Event name	tmnxFPResourcePolicyModified
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.233
Default severity	minor
Source stream	main
Message format string	Class *$tmnxHwClass$* : Card : FP resource policy changed, the configuration must be saved and the system rebooted immediately
Cause	The FP resource policy applied to the FP has been modified, or a different FP resource policy is applied to the FP.
Effect	Modifying the configuration could result in a failure to instantiate queues.
Recovery	The configuration must be saved and the system rebooted immediately.

12.195 tmnxFPResourcePolicyModifiedClr

Table 349: tmnxFPResourcePolicyModifiedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2223
Event name	tmnxFPResourcePolicyModifiedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.234
Default severity	minor
Source stream	main
Message format string	Class *$tmnxHwClass$* : Card : alarm *$tmnxFPResourcePolicyModified $* cleared

Property name	Value
Cause	Generates a notification when tmnxFPResourcePolicyModified is cleared.
Effect	None.
Recovery	None.

12.196 tmnxFPResOversubscribed

Table 350: tmnxFPResOversubscribed properties

Property name	Value
Application name	CHASSIS
Event ID	2246
Event name	tmnxFPResOversubscribed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.263
Default severity	major
Source stream	main
Message format string	Card *$tmnxCardSlotNum$* FP *$tmnxFPNum$* resources oversubscribed: *$tFPResOversub$*
Cause	The tmnxFPResOversubscribed notification is generated when one or more of the FP resources have been oversubscribed.
Effect	Usage beyond limits can result in the system dropping packets which may cause degradation in service quality.
Recovery	Reduce traffic load and/or conjestion on the system. More specific action might be required depending on the specific oversubscription.

12.197 tmnxFPResOversubscribedCleared

Table 351: tmnxFPResOversubscribedCleared properties

Property name	Value
Application name	CHASSIS
Event ID	2247
Event name	tmnxFPResOversubscribedCleared
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.264
Default severity	cleared
Source stream	main
Message format string	Card *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFabricSlotNum$* resources no longer oversubscribed
Cause	The tmnxFPResOversubscribedCleared notification is generated when none of the FP resources are oversubscribed.
Effect	The system returns to normal mode of operation and can service all the received traffic in the configured manner.
Recovery	There is no recovery for this notification.

12.198 tmnxGnssAcquiredFix

Table 352: tmnxGnssAcquiredFix properties

Property name	Value
Application name	CHASSIS
Event ID	2189
Event name	tmnxGnssAcquiredFix
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.180
Default severity	minor
Source stream	main
Message format string	GNSS Receiver - position fix obtained
Cause	The tmnxGnssAcquiredFix notification is generated when the GNSS receiver has acquired a valid fix on its position.

Property name	Value
Effect	The position of the system is known.
Recovery	None needed

12.199 tmnxGnssAcquiringFix

Table 353: tmnxGnssAcquiringFix properties

Property name	Value
Application name	CHASSIS
Event ID	2188
Event name	tmnxGnssAcquiringFix
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.179
Default severity	minor
Source stream	main
Message format string	GNSS Receiver - attempting to acquire a position fix
Cause	The tmnxGnssAcquiringFix notification is generated when the GNSS receiver starts to acquire a fix. This occurs when the GNSS receiver is enabled, and also when the GNSS receiver loses its fix.
Effect	The position of the system is unknown until the receiver acquires a fix.
Recovery	Ensure that the GNSS antenna is properly connected to the system.

12.200 tmnxHwAggShpSchedEventOvrflw

Table 354: tmnxHwAggShpSchedEventOvrflw properties

Property name	Value
Application name	CHASSIS
Event ID	2243
Event name	tmnxHwAggShpSchedEventOvrflw

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.260
Default severity	minor
Source stream	main
Message format string	Hw Agg Shaped Sched log event overflow occurred on card *$tmnx ChassisNotifyCardSlotNum$* at *$tmnxHwAggShpTimeEventOccured$*
Cause	The tmnxHwAggShpSchedEventOvrflwClr notification is generated when HW Agg Shaper Scheduler oper color occurs more than 200 times because of Number of agg-shapers parented to a scheduler. The IOM raises the final trap to indicate overflow and stops logging traps.
Effect	Hw Agg shaper scheduler color notifications on the card may not be received.
Recovery	Notifications will resume once the Overflow clear is set.

12.201 tmnxHwAggShpSchedEventOvrflwClr

Table 355: tmnxHwAggShpSchedEventOvrflwClr properties

Property name	Value
Application name	CHASSIS
Event ID	2242
Event name	tmnxHwAggShpSchedEventOvrflwClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.259
Default severity	minor
Source stream	main
Message format string	*$tmnxHwAggShpMissingNotifCount$* HW Agg Shaper Sched events were dropped in the last event throttling interval on card *$tmnxChassis NotifyCardSlotNum$* at *$tmnxHwAggShpTimeEventOccured$*
Cause	The tmnxHwAggShpSchedEventOvrflwClr notification is generated when the CPM polls the IOM for Hw Agg Shaper Sched 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.

12.202 tmnxInterChassisCommsDown

Table 356: 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
Source stream	main
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.

12.203 tmnxInterChassisCommsUp

Table 357: tmnxInterChassisCommsUp properties

Property name	Value
Application name	CHASSIS
Event ID	4002
Event name	tmnxInterChassisCommsUp

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxInterChassis Notifications.2
Default severity	critical
Source stream	main
Message format string	Control communications established between the active CPM and the chassis
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

12.204 tmnxIomEventOverflow

Table 358: 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
Source stream	main
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.

Property name	Value
Effect	Some FP notifications configured on the card may not be received.
Recovery	Notifications will resume once the Overflow clear is set.

12.205 tmnxIomEventOverflowClr

Table 359: 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
Source stream	main
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.

12.206 tmnxIomResExhausted

Table 360: tmnxIomResExhausted properties

Property name	Value
Application name	CHASSIS

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

12.207 tmnxIomResHighLimitReached

Table 361: 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
Source stream	main
Message format string	The *$tmnxIomResourceType$* resources on IOM *$tmnxChassisNotify CardSlotNum$* 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.

Property name	Value
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.

12.208 tmnxIomResStateClr

Table 362: tmnxIomResStateClr properties

Property name	Value
Application name	CHASSIS
Event ID	2123
Event name	tmnxIomResStateClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.110
Default severity	minor
Source stream	main
Message format string	The *$tmnxIomResourceType$* resources on IOM *$tmnxChassisNotify CardSlotNum$* 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.

12.209 tmnxIomRsrcEventOverflow

Table 363: tmnxIomRsrcEventOverflow properties

Property name	Value
Application name	CHASSIS
Event ID	3257
Event name	tmnxIomRsrcEventOverflow
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.257
Default severity	warning
Source stream	main
Message format string	A resource event overflow occurred on card *$tmnxChassisNotifyCard SlotNum$* at *$tmnxIomRsrcTimeEventOccured$*.
Cause	The tmnxIomRsrcEventOverflow notification is generated when tmnx IomRsrcUsageHighLimitReached, tmnxIomRsrcUsageExhausted, tmnxIomRsrcUsageRecovered, tmnxIomRsrcOwnerOversubscribed, or tmnxIomRsrcOwnerOversubscrbdClr 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 IOM notifications may not be received.
Recovery	Notifications will resume once the Overflow clear is set.

12.210 tmnxIomRsrcEventOverflowClr

Table 364: tmnxIomRsrcEventOverflowClr properties

Property name	Value
Application name	CHASSIS
Event ID	3258
Event name	tmnxIomRsrcEventOverflowClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.258
Default severity	minor
Source stream	main

Property name	Value
Message format string	*$tmnxIomRsrcMissingNotifCount$* resource events were dropped in the last event throttling interval on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxIomRsrcTimeEventOccured$*.
Cause	The tmnxIomRsrcEventOverflowClr 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.

12.211 tmnxIomRsrcOwnerOversubscrbdClr

Table 365: tmnxIomRsrcOwnerOversubscrbdClr properties

Property name	Value
Application name	CHASSIS
Event ID	3260
Event name	tmnxIomRsrcOwnerOversubscrbdClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.262
Default severity	minor
Source stream	main
Message format string	The *$tmnxIomRsrcResourceType$* resources needed by *$tmnxIom RsrcOwnerType$* on card *$tmnxChassisNotifyCardSlotNum$* have been satisfied at *$tmnxIomRsrcTimeEventOccured$*. All *$tmnxIomRsrc OwnerType$* traffic can flow.
Cause	The tmnxIomRsrcOwnerOversubscrbdClr notification is generated when all the required IOM resources of type tmnxIomRsrcResource Type for owner tmnxIomRsrcOwnerType have been allocated.
Effect	Traffic for owner tmnxIomRsrcOwnerType is no longer affected.
Recovery	There is no recovery for this notification.

12.212 tmnxIomRsrcOwnerOversubscribed

Table 366: tmnxIomRsrcOwnerOversubscribed properties

Property name	Value
Application name	CHASSIS
Event ID	3259
Event name	tmnxIomRsrcOwnerOversubscribed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.261
Default severity	major
Source stream	main
Message format string	The *$tmnxIomRsrcResourceType$* resources needed by *$tmnxIomRsrcOwnerType$* on card *$tmnxChassisNotifyCardSlotNum$* are oversubscribed at *$tmnxIomRsrcTimeEventOccured$*. Some *$tmnxIomRsrcOwnerType$* traffic may not flow.
Cause	The tmnxIomRsrcOwnerOversubscribed notification is generated when the IOM resource of type tmnxIomRsrcResourceType has been exhausted for owner tmnxIomRsrcOwnerType.
Effect	Traffic for owner tmnxIomRsrcOwnerType may be affected.
Recovery	Intervention may be required to recover resources.

12.213 tmnxIomRsrcUsageExhausted

Table 367: tmnxIomRsrcUsageExhausted properties

Property name	Value
Application name	CHASSIS
Event ID	3253
Event name	tmnxIomRsrcUsageExhausted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.253
Default severity	critical

Property name	Value
Source stream	main
Message format string	Possible messages: • The *$tmnxIomRsrcResourceType$* resources on card *$tmnx ChassisNotifyCardSlotNum$* Forwarding Plane *$tmnxChassisNotify FpNum$* have been exhausted at *$tmnxIomRsrcTimeEventOccured $*. • The *$tmnxIomRsrcResourceType$* resources on card *$tmnx ChassisNotifyCardSlotNum$* Forwarding Plane *$tmnxChassisNotify FpNum$* have been exhausted at *$tmnxIomRsrcTimeEventOccured $*. Current utilization is *$tmnxIomRsrcUsagePercent$*%%.
Cause	The tmnxIomRsrcUsageExhausted notification is generated when all the IOM resources of type tmnxIomRsrcResourceType have been exhausted.
Effect	The specified IOM resource has reached its limit. Some traffic may be affected.
Recovery	Intervention may be required to recover resources.

12.214 tmnxIomRsrcUsageHighLimitReached

Table 368: tmnxIomRsrcUsageHighLimitReached properties

Property name	Value
Application name	CHASSIS
Event ID	3252
Event name	tmnxIomRsrcUsageHighLimitReached
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.252
Default severity	warning
Source stream	main
Message format string	Possible messages: • The *$tmnxIomRsrcResourceType$* resources on card *$tmnx ChassisNotifyCardSlotNum$* Forwarding Plane *$tmnxChassisNotify FpNum$* have reached or exceeded the high utilization threshold at *$tmnxIomRsrcTimeEventOccured$*. • The *$tmnxIomRsrcResourceType$* resources on card *$tmnx ChassisNotifyCardSlotNum$* Forwarding Plane *$tmnxChassisNotify*

Property name	Value
	FpNum$* have reached or exceeded the high utilization threshold at *$tmnxIomRsrcTimeEventOccured$*. Current utilization is *$tmnxIomRsrcUsagePercent$%%.
Cause	The tmnxIomRsrcUsageHighLimitReached notification is generated when the utilization of the IOM resource of type tmnxIomRsrcResourceType reaches or exceeds the high utilization threshold.
Effect	The specified IOM resource is getting close to exhaustion.
Recovery	There is no recovery required for this notification.

12.215 tmnxIomRsrcUsageRecovered

Table 369: tmnxIomRsrcUsageRecovered properties

Property name	Value
Application name	CHASSIS
Event ID	3254
Event name	tmnxIomRsrcUsageRecovered
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.254
Default severity	minor
Source stream	main
Message format string	Possible messages: • The *$tmnxIomRsrcResourceType$* resources on card *$tmnxChassisNotifyCardSlotNum$* Forwarding Plane *$tmnxChassisNotifyFpNum$* have dropped below the warning utilization threshold at *$tmnxIomRsrcTimeEventOccured$*. • The *$tmnxIomRsrcResourceType$* resources on card *$tmnxChassisNotifyCardSlotNum$* Forwarding Plane *$tmnxChassisNotifyFpNum$* have dropped below the warning utilization threshold at *$tmnxIomRsrcTimeEventOccured$*. Current utilization is *$tmnxIomRsrcUsagePercent$*%%.
Cause	The tmnxIomRsrcUsageRecovered notification is generated when the utilization of the IOM resource of type tmnxIomRsrcResourceType drops below the warning threshold.

Property name	Value
Effect	The utilization of the specified IOM resource has dropped below the warning threshold.
Recovery	There is no recovery required for this notification.

12.216 tmnxIPMacCpmFilterOverload

Table 370: tmnxIPMacCpmFilterOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2183
Event name	tmnxIPMacCpmFilterOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.172
Default severity	critical
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an IPv4 or MAC CPM Filter in overload.
Cause	The tmnxIPMacCpmFilterOverload notification is generated when an IPv4 or MAC CPM Filter policy is in overload on an FP.
Effect	The impacted IPv4 or MAC CPM Filter policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted IPv4 or MAC CPM Filter policy, policy entries, and FPs using the appropriate tools commands. Remove or modify policy entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.217 tmnxIPMacCpmFilterOverloadClear

Table 371: tmnxIPMacCpmFilterOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2184
Event name	tmnxIPMacCpmFilterOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.173
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an IPv4 or MAC CPM Filter in overload.
Cause	The tmnxIPMacCpmFilterOverloadClear notification is generated when IPv4 or MAC CPM Filter policies are no longer in overload on an FP.
Effect	The IPv4 or MAC CPM Filter policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.218 tmnxIPMacFilterEgrNearFull

Table 372: tmnxIPMacFilterEgrNearFull properties

Property name	Value
Application name	CHASSIS
Event ID	2277
Event name	tmnxIPMacFilterEgrNearFull
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.199
Default severity	minor
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has egress IPv4 or MAC ACL Filters at near full utilization.

Property name	Value
Cause	The tmnxIPMacFilterEgrNearFull notification is generated when an egress IPv4 or MAC ACL Filter policies are near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.219 tmnxIPMacFilterEgrNearFullClear

Table 373: tmnxIPMacFilterEgrNearFullClear properties

Property name	Value
Application name	CHASSIS
Event ID	2278
Event name	tmnxIPMacFilterEgrNearFullClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.200
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has egress IPv4 or MAC ACL Filters near full utilization.
Cause	The tmnxIPMacFilterEgrNearFullClear notification is generated when egress IPv4 or MAC ACL Filter policies are no longer near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.220 tmnxIPMacFilterEgrOverload

Table 374: tmnxIPMacFilterEgrOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2177
Event name	tmnxIPMacFilterEgrOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.166
Default severity	critical
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an egress IPv4 or MAC ACL Filter in overload.
Cause	The tmnxIPMacFilterEgrOverload notification is generated when an egress IPv4 or MAC ACL Filter policy is in overload on an FP.
Effect	The impacted egress IPv4 or MAC ACL Filter policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted egress IPv4 or MAC ACL Filter policy, policy entries, and FPs using the appropriate tools commands. Remove or modify policy entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.221 tmnxIPMacFilterEgrOverloadClear

Table 375: tmnxIPMacFilterEgrOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2178
Event name	tmnxIPMacFilterEgrOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.167
Default severity	cleared
Source stream	main

Property name	Value
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an egress IPv4 or MAC ACL Filter in overload.
Cause	The tmnxIPMacFilterEgrOverloadClear notification is generated when egress IPv4 or MAC ACL Filter policies are no longer in overload on an FP.
Effect	The egress IPv4 or MAC ACL Filter policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.222 tmnxIPMacFilterIngNearFull

Table 376: tmnxIPMacFilterIngNearFull properties

Property name	Value
Application name	CHASSIS
Event ID	2275
Event name	tmnxIPMacFilterIngNearFull
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.197
Default severity	minor
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has ingress IPv4 or MAC ACL Filters at near full utilization.
Cause	The tmnxIPMacFilterIngNearFull notification is generated when an ingress IPv4 or MAC ACL Filter policies are near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.223 tmnxIPMacFilterIngNearFullClear

Table 377: tmnxIPMacFilterIngNearFullClear properties

Property name	Value
Application name	CHASSIS
Event ID	2276
Event name	tmnxIPMacFilterIngNearFullClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.198
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has ingress IPv4 or MAC ACL Filters at near full utilization.
Cause	The tmnxIPMacFilterIngNearFullClear notification is generated when ingress IPv4 or MAC ACL Filter policies are no longer near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.224 tmnxIPMacFilterIngOverload

Table 378: tmnxIPMacFilterIngOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2175
Event name	tmnxIPMacFilterIngOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.164
Default severity	critical
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an ingress IPv4 or MAC ACL Filter in overload.

Property name	Value
Cause	The tmnxIPMacFilterIngOverload notification is generated when an ingress IPv4 or MAC ACL Filter policy is in overload on an FP.
Effect	The impacted ingress IPv4 or MAC ACL Filter policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted ingress IPv4 or MAC ACL Filter policy, policy entries, and FPs using the appropriate tools commands. Remove or modify policy entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.225 tmnxIPMacFilterIngOverloadClear

Table 379: tmnxIPMacFilterIngOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2176
Event name	tmnxIPMacFilterIngOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.165
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an ingress IPv4 or MAC ACL Filter in overload.
Cause	The tmnxIPMacFilterIngOverloadClear notification is generated when ingress IPv4 or MAC ACL Filter policies are no longer in overload on an FP.
Effect	The ingress IPv4 or MAC ACL Filter policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.226 tmnxIPMacQosIngOverload

Table 380: tmnxIPMacQosIngOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2167
Event name	tmnxIPMacQosIngOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.156
Default severity	major
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotify FpNum$* has an ingress QoS policy with IPv4 or MAC criteria entries in overload.
Cause	The tmnxIPMacQosIngOverload notification is generated when an ingress QoS policy is in overload on an FP due to its configured IPv4 or MAC criteria entries.
Effect	The impacted IPv4 or MAC criteria entries in the ingress QoS policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted ingress QoS policy, policy entries, and FPs using the appropriate tools commands. Remove or modify the policy criteria entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.227 tmnxIPMacQosIngOverloadClear

Table 381: tmnxIPMacQosIngOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2168
Event name	tmnxIPMacQosIngOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.157
Default severity	cleared

Property name	Value
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an ingress QoS policy with IPv4 or MAC criteria entries in overload.
Cause	The tmnxIPMacQosIngOverloadClear notification is generated when ingress QoS policies are no longer in overload on an FP.
Effect	The IPv4 or MAC criteria entries in the ingress QoS policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.228 tmnxIPQosEgrOverload

Table 382: tmnxIPQosEgrOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2169
Event name	tmnxIPQosEgrOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.158
Default severity	major
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an egress QoS policy with IPv4 criteria entries in overload.
Cause	The tmnxIPQosEgrOverload notification is generated when an egress QoS policy is in overload on an FP due to its configured IPv4 criteria entries.
Effect	The impacted IPv4 criteria entries in the egress QoS policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted egress QoS policy, policy entries, and FPs using the appropriate tools commands. Remove or modify the policy criteria entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.229 tmnxIPQosEgrOverloadClear

Table 383: tmnxIPQosEgrOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2170
Event name	tmnxIPQosEgrOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.159
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum$* no longer has an egress QoS policy with IPv4 criteria entries in overload.
Cause	The tmnxIPQosEgrOverloadClear notification is generated when egress QoS policies are no longer in overload on an FP.
Effect	The IPv4 criteria entries in the egress QoS policy on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.230 tmnxIPsecIsaGrpActiveIsaChgd

Table 384: 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

Property name	Value
Source stream	main
Message format string	Active ISA changed to *$tmnxIPsecIsaGrpActiveIsa$* for IPsec ISA group *$tmnxIPsecIsaGrpId$* where primary ISA is *$tmnxIPsecIsaGrp PrimaryIsa$* 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

12.231 tmnxIPsecIsaGrpTnlHighWMark

Table 385: 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
Source stream	main
Message format string	Number of tunnels for an IPsec ISA module for the group *$tmnxIPsec IsaGrpId$* 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

12.232 tmnxIPsecIsaGrpTnlLowWMark

Table 386: 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
Source stream	main
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.
Effect	N/A
Recovery	N/A

12.233 tmnxIPsecIsaGrpTnlMax

Table 387: 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

Property name	Value
Source stream	main
Message format string	Number of tunnels for an IPsec ISA module for the group *$tmnxIPsecIsaGrpId$* has reached the maximum limit *$tmnxIPsecIsaGrpMaxTunnels$*.
Cause	The number of tunnels for an IPsec ISA (Integrated Service Adaptor) module has reached the maximum limit.
Effect	N/A
Recovery	N/A

12.234 tmnxIPsecIsaGrpUnableToSwitch

Table 388: 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
Source stream	main
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.

12.235 tmnxIPv6CpmFilterOverload

Table 389: tmnxIPv6CpmFilterOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2185
Event name	tmnxIPv6CpmFilterOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.174
Default severity	critical
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an IPv6 CPM Filter in overload.
Cause	The tmnxIPv6CpmFilterOverload notification is generated when an IPv6 CPM Filter policy is in overload on an FP.
Effect	The impacted IPv6 CPM Filter policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted IPv6 CPM Filter policy, policy entries, and FPs using the appropriate tools commands. Remove or modify policy entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.236 tmnxIPv6CpmFilterOverloadClear

Table 390: tmnxIPv6CpmFilterOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2186
Event name	tmnxIPv6CpmFilterOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.175
Default severity	cleared
Source stream	main

Property name	Value
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum$* no longer has an IPv6 CPM Filter in overload.
Cause	The tmnxIPv6CpmFilterOverloadClear notification is generated when IPv6 CPM Filter policies are no longer in overload on an FP.
Effect	The IPv6 CPM Filter policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.237 tmnxIPv6FilterEgrNearFull

Table 391: tmnxIPv6FilterEgrNearFull properties

Property name	Value
Application name	CHASSIS
Event ID	2281
Event name	tmnxIPv6FilterEgrNearFull
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.203
Default severity	minor
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum$* has egress IPv6 ACL Filters at near full utilization.
Cause	The tmnxIPv6FilterEgrNearFull notification is generated when an egress IPv6 ACL Filter policies are near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.238 tmnxIPv6FilterEgrNearFullClear

Table 392: tmnxIPv6FilterEgrNearFullClear properties

Property name	Value
Application name	CHASSIS
Event ID	2282
Event name	tmnxIPv6FilterEgrNearFullClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.204
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum$* no longer has egress IPv6 ACL Filters at near full utilization.
Cause	The tmnxIPv6FilterEgrNearFullClear notification is generated when egress IPv6 ACL Filter policies are no longer near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.239 tmnxIPv6FilterEgrOverload

Table 393: tmnxIPv6FilterEgrOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2181
Event name	tmnxIPv6FilterEgrOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.170
Default severity	critical
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum$* has an egress IPv6 ACL Filter in overload.

Property name	Value
Cause	The tmnxIPv6FilterEgrOverload notification is generated when an egress IPv6 ACL Filter policy is in overload on an FP.
Effect	The impacted egress IPv6 ACL Filter policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted egress IPv6 ACL Filter policy, policy entries, and FPs using the appropriate tools commands. Remove or modify policy entries or changed the policy assigned to the impacted FPs until the overload condition is cleared.

12.240 tmnxIPv6FilterEgrOverloadClear

Table 394: tmnxIPv6FilterEgrOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2182
Event name	tmnxIPv6FilterEgrOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.171
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an egress IPv6 ACL Filter in overload.
Cause	The tmnxIPv6FilterEgrOverloadClear notification is generated when egress IPv6 ACL Filter policies are no longer in overload on an FP.
Effect	The egress IPv6 ACL Filter policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.241 tmnxIPv6FilterIngNearFull

Table 395: tmnxIPv6FilterIngNearFull properties

Property name	Value
Application name	CHASSIS
Event ID	2279
Event name	tmnxIPv6FilterIngNearFull
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.201
Default severity	minor
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has ingress IPv6 ACL Filters at near full utilization.
Cause	The tmnxIPv6FilterIngNearFull notification is generated when an ingress IPv6 ACL Filter policies are near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.242 tmnxIPv6FilterIngNearFullClear

Table 396: tmnxIPv6FilterIngNearFullClear properties

Property name	Value
Application name	CHASSIS
Event ID	2280
Event name	tmnxIPv6FilterIngNearFullClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.202
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has ingress IPv6 ACL Filters at near full utilization.

Property name	Value
Cause	The tmnxIPv6FilterIngNearFullClear notification is generated when ingress IPv6 ACL Filter policies are no longer near full utilization on an FP.
Effect	There is no operational impact due to this event.
Recovery	None required.

12.243 tmnxIPv6FilterIngOverload

Table 397: tmnxIPv6FilterIngOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2179
Event name	tmnxIPv6FilterIngOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.168
Default severity	critical
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an ingress IPv6 ACL Filter in overload.
Cause	The tmnxIPv6FilterIngOverload notification is generated when an ingress IPv6 ACL Filter policy is in overload on a FP.
Effect	The impacted ingress IPv6 ACL Filter policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted ingress IPv6 ACL Filter policy, policy entries, and FPs using the appropriate tools commands. Remove or modify policy entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.244 tmnxIPv6FilterIngOverloadClear

Table 398: tmnxIPv6FilterIngOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2180
Event name	tmnxIPv6FilterIngOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.169
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an ingress IPv6 ACL Filter in overload.
Cause	The tmnxIPv6FilterIngOverloadClear notification is generated when ingress IPv6 ACL Filter policies are no longer in overload on an FP.
Effect	The ingress IPv6 ACL Filter policies on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.245 tmnxIPv6QosEgrOverload

Table 399: tmnxIPv6QosEgrOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2173
Event name	tmnxIPv6QosEgrOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.162
Default severity	major
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* has an egress QoS policy with IPv6 criteria entries in overload.

Property name	Value
Cause	The tmnxIPv6QosEgrOverload notification is generated when an egress QoS policy is in overload on an FP due to its configured IPv6 criteria entries.
Effect	The impacted IPv6 criteria entries in the egress QoS Policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted egress QoS policy, policy entries, and FPs using the appropriate tools commands. Remove or modify the policy criteria entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.246 tmnxIPv6QosEgrOverloadClear

Table 400: tmnxIPv6QosEgrOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2174
Event name	tmnxIPv6QosEgrOverloadClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.163
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an egress QoS policy with IPv6 criteria entries in overload.
Cause	The tmnxIPv6QosEgrOverloadClear notification is generated when egress QoS policies are no longer in overload on an FP.
Effect	The IPv6 criteria entries in the egress QoS policy on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.247 tmnxIPv6QosIngOverload

Table 401: tmnxIPv6QosIngOverload properties

Property name	Value
Application name	CHASSIS
Event ID	2171
Event name	tmnxIPv6QosIngOverload
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.160
Default severity	major
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum$* has an ingress QoS policy with IPv6 criteria entries in overload.
Cause	The tmnxIPv6QosIngOverload notification is generated when an ingress QoS policy is in overload on an FP due to its configured IPv6 criteria entries.
Effect	The impacted IPv6 criteria entries in the ingress QoS policy on the affected FP will not work as expected, because not all entries are programmed.
Recovery	Identify the impacted ingress QoS policy, policy entries, and FPs using the appropriate tools commands. Remove or modify the policy criteria entries or change the policy assigned to the impacted FPs until the overload condition is cleared.

12.248 tmnxIPv6QosIngOverloadClear

Table 402: tmnxIPv6QosIngOverloadClear properties

Property name	Value
Application name	CHASSIS
Event ID	2172
Event name	tmnxIPv6QosIngOverloadClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.161
Default severity	cleared
Source stream	main
Message format string	Slot *$tmnxChassisNotifyCardSlotNum$* FP *$tmnxChassisNotifyFpNum $* no longer has an ingress QoS policy with IPv6 criteria entries in overload.
Cause	The tmnxIPv6QosIngOverloadClear notification is generated when ingress QoS policies are no longer in overload on an FP.
Effect	The IPv6 criteria entries in the ingress QoS policy on the affected FP will work as expected, because all entries are programmed.
Recovery	No recovery required.

12.249 tmnxIxrResourceExhausted

Table 403: tmnxIxrResourceExhausted properties

Property name	Value
Application name	CHASSIS
Event ID	2433
Event name	tmnxIxrResourceExhausted
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.298
Default severity	critical
Source stream	main
Message format string	The *$tmnxNotifIxrResource$* resources have been exhausted.
Cause	The tmnxIxrResourceExhausted notification is generated when the utilization of the resource specified by tmnxNotifIxrResource has reached its limit.
Effect	The utilization of the specified resource has reached its limit.
Recovery	Intervention may be required to recover resources.

12.250 tmnxIxrResourceExhaustedByOwner

Table 404: tmnxIxrResourceExhaustedByOwner properties

Property name	Value
Application name	CHASSIS
Event ID	2436
Event name	tmnxIxrResourceExhaustedByOwner
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.301
Default severity	critical
Source stream	main
Message format string	The *$tmnxNotifIxrResource$* resources needed by *$tmnxNotifIxr ResourceOwner$* have been exhausted. Some *$tmnxNotifIxrResource Owner$* traffic may be affected.
Cause	The tmnxIxrResourceExhaustedByOwner notification is generated when the utilization of the resource specified by tmnxNotifIxrResource reached its limit for application specified by tmnxNotifIxrResource Owner.
Effect	Usage of the resource specified by tmnxNotifIxrResource reached its limit for application specified by tmnxNotifIxrResourceOwner.
Recovery	Intervention may be required to recover resources.

12.251 tmnxIxrResourceHighUsage

Table 405: tmnxIxrResourceHighUsage properties

Property name	Value
Application name	CHASSIS
Event ID	2432
Event name	tmnxIxrResourceHighUsage
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.297

Property name	Value
Default severity	major
Source stream	main
Message format string	The *$tmnxNotifIxrResource$* resources have reached or exceeded the high utilization threshold. Current utilization is *$tmnxNotifIxrRsrcUtil Percentage$*%%.
Cause	The tmnxIxrResourceHighUsage notification is generated when the number of allocated resources reaches or exceeds the warning high limit.
Effect	The specified resource is getting close to exhaustion.
Recovery	There is no recovery required for this notification.

12.252 tmnxIxrResourceHighUsageByOwner

Table 406: tmnxIxrResourceHighUsageByOwner properties

Property name	Value
Application name	CHASSIS
Event ID	2435
Event name	tmnxIxrResourceHighUsageByOwner
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.300
Default severity	major
Source stream	main
Message format string	The *$tmnxNotifIxrResource$* resources needed by *$tmnxNotifIxr ResourceOwner$* have reached or exceeded the high utilization threshold. Current utilization is *$tmnxNotifIxrRsrcUtilPercentage$*%%.
Cause	The tmnxIxrResourceHighUsageByOwner notification is generated when the number of allocated resources by an owner reaches or exceeds the warning high limit.
Effect	The specified application is getting close to its maximal usage of the specified resource.
Recovery	There is no recovery required for this notification.

12.253 tmnxIxrResourceRecovered

Table 407: tmnxIxrResourceRecovered properties

Property name	Value
Application name	CHASSIS
Event ID	2434
Event name	tmnxIxrResourceRecovered
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.299
Default severity	minor
Source stream	main
Message format string	The *$tmnxNotifIxrResource$* resources have dropped below the warning utilization threshold. Current utilization is *$tmnxNotifIxrRsrcUtilPercentage$*%%.
Cause	The tmnxIxrResourceRecovered notification is generated when the number of allocated resources drops below the warning threshold. This trap is generated only if the tmnxIxrResourceHighUsage notification or the tmnxIxrResourceExhausted notification had been generated.
Effect	The utilization of the specified resource has dropped below the warning threshold.
Recovery	There is no recovery required for this notification.

12.254 tmnxIxrResourceRecoveredByOwner

Table 408: tmnxIxrResourceRecoveredByOwner properties

Property name	Value
Application name	CHASSIS
Event ID	2437
Event name	tmnxIxrResourceRecoveredByOwner
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.302

Property name	Value
Default severity	minor
Source stream	main
Message format string	The *$tmnxNotifIxrResource$* resources needed by *$tmnxNotifIxr ResourceOwner$* have dropped below the warning utilization threshold. Current utilization is *$tmnxNotifIxrResourceOwner$*%%.
Cause	The tmnxIxrResourceRecoveredByOwner notification is generated when the number of allocated resources by the specified application drops below the warning threshold. This trap is generated only if the tmnxIxrResourceHighUsageByOwner notification or the tmnxIxr ResourceExhaustedByOwner notification had been generated.
Effect	The utilization of the specified resource by a given application has dropped below the warning threshold.
Recovery	There is no recovery required for this notification.

12.255 tmnxMDAIsaTunnelGroupChange

Table 409: 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
Source stream	main
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

12.256 tmnxPeBootloaderVersionMismatch

Table 410: 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
Source stream	main
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

12.257 tmnxPeBootromVersionMismatch

Table 411: tmnxPeBootromVersionMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2028
Event name	tmnxPeBootromVersionMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.36

Property name	Value
Default severity	major
Source stream	main
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

12.258 tmnxPeFirmwareVersionWarning

Table 412: 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	warning
Source stream	main
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

12.259 tmnxPeFPGAVersionMismatch

Table 413: 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
Source stream	main
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

12.260 tmnxPeKernelVersionMismatch

Table 414: tmnxPeKernelVersionMismatch properties

Property name	Value
Application name	CHASSIS
Event ID	2221
Event name	tmnxPeKernelVersionMismatch
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.232
Default severity	major

Property name	Value
Source stream	main
Message format string	Class *$tmnxHwClass$* : Kernel version mismatch - expected software version *$tmnxHwSoftwareCodeVersion$*, equipped version *$tmnx ChassisNotifyMismatchedVer$*
Cause	This notification is generated when there is a mismatch between the software version of the host kernel software and the CPM software. This may occur if the user updates the system software without following the recommended software upgrade procedures. The object tmnxChassisNotifyHwIndex identifies the CPM card. The object tmnx ChassisNotifyMismatchedVer contains the version of the host kernel software and tmnxHwSoftwareCodeVersion contains the version of the CPM software. This notification is only applicable to systems that use both host kernel software and CPM software, such as the 7705 SAR-Hm and the 7250 IXR-s.
Effect	Although the system may appear to work properly, the behavior of the system in this state is undefined. Using mismatched versions of host kernel software and CPM software is not supported.
Recovery	Follow the recommended software upgrade procedures to update the host kernel software and CPM software to the desired software release.

12.261 tmnxPeSoftwareLoadFailed

Table 415: 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
Source stream	main
Message format string	Class *$tmnxHwClass$* : Failed to load software from *$tmnxChassis NotifySoftwareLocation$*

Property name	Value
Cause	Generated when the CPM fails to load the software from a specified location. tmnxChassisNotifyHwIndex identifies the card for which the software load failed and tmnxChassisNotifySoftwareLocation contains the location from where the software load was attempted.
Effect	N/A
Recovery	N/A

12.262 tmnxPeSoftwareVersionMismatch

Table 416: 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
Source stream	main
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

12.263 tmnxPhysChassisFilterDoorClosed

Table 417: tmnxPhysChassisFilterDoorClosed properties

Property name	Value
Application name	CHASSIS
Event ID	2195
Event name	tmnxPhysChassisFilterDoorClosed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.194
Default severity	cleared
Source stream	main
Message format string	Filter door is closed
Cause	The tmnxPhysChassisFilterDoorClosed notification is generated when the filter door is present and closed.
Effect	The power shelves are protected by the closed door.
Recovery	No recovery required.

12.264 tmnxPhysChassisFilterDoorOpen

Table 418: tmnxPhysChassisFilterDoorOpen properties

Property name	Value
Application name	CHASSIS
Event ID	2194
Event name	tmnxPhysChassisFilterDoorOpen
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.193
Default severity	minor
Source stream	main
Message format string	Filter door is missing or open
Cause	The tmnxPhysChassisFilterDoorOpen notification is generated when the filter door is either open or not present.
Effect	Power shelf protection may be compromised.

Property name	Value
Recovery	If the filter door is not installed, install it. Close the filter door.

12.265 tmnxPhysChassisPCMInputFeed

Table 419: tmnxPhysChassisPCMInputFeed properties

Property name	Value
Application name	CHASSIS
Event ID	2165
Event name	tmnxPhysChassisPCMInputFeed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.154
Default severity	minor
Source stream	main
Message format string	Chassis *$tmnxPhysChassisNum$* pcm *$tmnxPhysChassisPCMId$* *$tmnxPhysChassisPCMInFeedDown$*not supplying power.
Cause	The tmnxPhysChassisPCMInputFeed notification is generated if any one of the input feeds for a given PCM has gone offline.
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.

12.266 tmnxPhysChassisPCMInputFeedClr

Table 420: tmnxPhysChassisPCMInputFeedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2166
Event name	tmnxPhysChassisPCMInputFeedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.155

Property name	Value
Default severity	cleared
Source stream	main
Message format string	The input feeds for chassis *$tmnxPhysChassisNum$* pcm *$tmnxPhysChassisPCMId$* are supplying power.
Cause	The tmnxPhysChassisPCMInputFeedClr notification is generated when the last of the missing input feeds for a given PCM has been brought back online.
Effect	All PCM input feeds are supplying power.
Recovery	No recovery required.

12.267 tmnxPhysChassisPMInputFeed

Table 421: tmnxPhysChassisPMInputFeed properties

Property name	Value
Application name	CHASSIS
Event ID	2192
Event name	tmnxPhysChassisPMInputFeed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.191
Default severity	minor
Source stream	main
Message format string	Power module *$tmnxHwIndex$ $tmnxPhysChassisPMInputFeedDown $*not supplying power.
Cause	The tmnxPhysChassisPMInputFeed notification is generated if any one of the input feeds for a given power module is not supplying power.
Effect	There is an increased risk of system power brownouts or blackouts.
Recovery	Restore all of the input feeds that are not supplying power.

12.268 tmnxPhysChassisPMInputFeedClr

Table 422: tmnxPhysChassisPMInputFeedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2193
Event name	tmnxPhysChassisPMInputFeedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.192
Default severity	cleared
Source stream	main
Message format string	The input feeds for power module *$tmnxHwIndex$* are supplying power.
Cause	The tmnxPhysChassPwrSupInputFeedClr notification is generated when the last of the missing input feeds has been brought back online.
Effect	All power module input feeds are supplying power.
Recovery	No recovery required.

12.269 tmnxPhysChassisPMOutFail

Table 423: tmnxPhysChassisPMOutFail properties

Property name	Value
Application name	CHASSIS
Event ID	2190
Event name	tmnxPhysChassisPMOutFail
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.189
Default severity	critical
Source stream	main
Message format string	Power module *$tmnxHwIndex$* output failure
Cause	The tmnxPhysChassisPMOutFail notification is generated when an output failure occurs on the power module.
Effect	The power module is no longer operational.

Property name	Value
Recovery	Insert a new power module.

12.270 tmnxPhysChassisPMOutFailClr

Table 424: tmnxPhysChassisPMOutFailClr properties

Property name	Value
Application name	CHASSIS
Event ID	2191
Event name	tmnxPhysChassisPMOutFailClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.190
Default severity	cleared
Source stream	main
Message format string	Power module *$tmnxHwIndex$* output failure cleared
Cause	The tmnxPhysChassisPMOutFailClr notification is generated when an output failure is cleared on the power module.
Effect	The power module is operational again.
Recovery	There is no recovery for this notification.

12.271 tmnxPhysChassisPMOverTemp

Table 425: tmnxPhysChassisPMOverTemp properties

Property name	Value
Application name	CHASSIS
Event ID	2196
Event name	tmnxPhysChassisPMOverTemp
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.195

Property name	Value
Default severity	critical
Source stream	main
Message format string	*$tmnxHwIndex$* over temperature
Cause	The tmnxPhysChassisPMOverTemp notification is generated when a power module's temperature surpasses the temperature threshold.
Effect	The power module is no longer operational.
Recovery	Check input feed and/or insert a new power module.

12.272 tmnxPhysChassisPMOverTempClr

Table 426: tmnxPhysChassisPMOverTempClr properties

Property name	Value
Application name	CHASSIS
Event ID	2197
Event name	tmnxPhysChassisPMOverTempClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.196
Default severity	cleared
Source stream	main
Message format string	*$tmnxHwIndex$* over temperature cleared
Cause	The tmnxPhysChassisPMOverTempClr notification is generated when a power module's temperature is reduced below the temperature threshold.
Effect	The power module is operational again.
Recovery	There is no recovery for this notification.

12.273 tmnxPhysChassPwrSupInputFeed

Table 427: tmnxPhysChassPwrSupInputFeed properties

Property name	Value
Application name	CHASSIS
Event ID	2159
Event name	tmnxPhysChassPwrSupInputFeed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.146
Default severity	minor
Source stream	main
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$ $tmnxPhysChassPowerSupInFeedDown$*not supplying power.
Cause	The tmnxPhysChassPwrSupInputFeed notification 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.

12.274 tmnxPhysChassPwrSupInputFeedClr

Table 428: tmnxPhysChassPwrSupInputFeedClr properties

Property name	Value
Application name	CHASSIS
Event ID	2160
Event name	tmnxPhysChassPwrSupInputFeedClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.147
Default severity	cleared
Source stream	main
Message format string	The input feeds for chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChassPowerSupId$* are supplying power.

Property name	Value
Cause	The tmnxPhysChassPwrSupInputFeedClr 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	No recovery required.

12.275 tmnxPhysChassPwrSupPemACRect

Table 429: tmnxPhysChassPwrSupPemACRect properties

Property name	Value
Application name	CHASSIS
Event ID	2157
Event name	tmnxPhysChassPwrSupPemACRect
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.144
Default severity	minor
Source stream	main
Message format string	Chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChass PowerSupId$ $tmnxPhysChassPowerSupPemACRect$*failed or missing.
Cause	The tmnxPhysChassPwrSupPemACRect notification 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.

12.276 tmnxPhysChassPwrSupPemACRectClr

Table 430: tmnxPhysChassPwrSupPemACRectClr properties

Property name	Value
Application name	CHASSIS
Event ID	2158
Event name	tmnxPhysChassPwrSupPemACRectClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.145
Default severity	cleared
Source stream	main
Message format string	The chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChassPowerSupId$* AC rectifiers are fully operational.
Cause	The tmnxPhysChassPwrSupPemACRectClr 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.
Recovery	No recovery required.

12.277 tmnxPhysChassPwrSupWrgFanDir

Table 431: tmnxPhysChassPwrSupWrgFanDir properties

Property name	Value
Application name	CHASSIS
Event ID	2155
Event name	tmnxPhysChassPwrSupWrgFanDir
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.142
Default severity	major
Source stream	main
Message format string	The *$tmnxPhysChassPowerSupFanDir$* fan direction for chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChassPowerSupId$* is not supported.

Property name	Value
Cause	The tmnxPhysChassPwrSupWrgFanDir 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.

12.278 tmnxPhysChassPwrSupWrgFanDirClr

Table 432: tmnxPhysChassPwrSupWrgFanDirClr properties

Property name	Value
Application name	CHASSIS
Event ID	2156
Event name	tmnxPhysChassPwrSupWrgFanDirClr
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.143
Default severity	cleared
Source stream	main
Message format string	The fan direction for chassis *$tmnxPhysChassisNum$* power supply *$tmnxPhysChassPowerSupId$* has been corrected.
Cause	The tmnxPhysChassPwrSupWrgFanDirClr 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.

12.279 tmnxPlcyAcctPlcrPoolExcResource

Table 433: tmnxPlcyAcctPlcrPoolExcResource properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2231
Event name	tmnxPlcyAcctPlcrPoolExcResource
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.242
Default severity	minor
Source stream	main
Message format string	Policer Resource usage on card *$tmnxCardSlotNum$* and forwarding plane *$tmnxFPNum$* exceeds 95 percent of the policer limit. Total policer resource used is '*$tmnxFPPlcyAcctPolicerInUse$*' and the limit is ' *$tmnxFPPlcyAcctPolicerLimit$*'
Cause	The tmnxPlcyAcctPlcrPoolExcResource notification is generated when the number of in-use policer resource usage as specified by tmnxFPPlcyAcctPolicerInUse exceeds 95 percent of the policer limit as specified by tmnxFPPlcyAcctPolicerLimit.
Effect	The affected device may not provide accurate and complete statistics.
Recovery	There is no recovery required for this notification.

12.280 tmnxPlcyAcctPlcrPoolLowResource

Table 434: tmnxPlcyAcctPlcrPoolLowResource properties

Property name	Value
Application name	CHASSIS
Event ID	2232
Event name	tmnxPlcyAcctPlcrPoolLowResource
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.243
Default severity	minor
Source stream	main
Message format string	Policer Resource usage on card *$tmnxCardSlotNum$* and forwarding plane *$tmnxFPNum$* is below 85 percent of the policer limit. Total policer resource used is '*$tmnxFPPlcyAcctPolicerInUse$*' and the limit is ' *$tmnxFPPlcyAcctPolicerLimit$*'

Property name	Value
Cause	The tmnxPlcyAcctPlcrPoolLowResource notification is generated when the number of in-use policer resource as specified by tmnxFPPlcyAcct PolicerInUse is below 85 percent of the policer limit as specified by tmnxFPPlcyAcctPolicerLimit.
Effect	The configured policer limit is cleared when the number of in-use policer resources falls below 85 percent of the policer limit.
Recovery	There is no recovery required for this notification.

12.281 tmnxPlcyAcctStatsEventOvrflw

Table 435: tmnxPlcyAcctStatsEventOvrflw properties

Property name	Value
Application name	CHASSIS
Event ID	2120
Event name	tmnxPlcyAcctStatsEventOvrflw
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.107
Default severity	minor
Source stream	main
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.

12.282 tmnxPlcyAcctStatsEventOvrflwClr

Table 436: 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
Source stream	main
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.

12.283 tmnxPlcyAcctStatsPoolExcResource

Table 437: 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
Source stream	main
Message format string	Stats Resource usage on card *$tmnxCardSlotNum$* and forwarding plane *$tmnxFPNum$* exceeds 95 percent of the stats pool limit. Total

Property name	Value
	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.

12.284 tmnxPlcyAcctStatsPoolLowResource

Table 438: 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
Source stream	main
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 ' *$tmnxFPPlcyAcctStatsPool$*'
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.

12.285 tmnxPowerShelfCommsDown

Table 439: tmnxPowerShelfCommsDown properties

Property name	Value
Application name	CHASSIS
Event ID	6002
Event name	tmnxPowerShelfCommsDown
SNMP notification prefix and OID	TIMETRA-POWER-SHELF-MIB.tmnxPowerShelfNotifications.2
Default severity	minor
Source stream	main
Message format string	*$tmnxHwIndex$* lost communication with *$tmnxCpmPowerShelf CommsFail$*
Cause	The tmnxPowerShelfCommsDown is generated when there is a loss of communications with the power shelf controller.
Effect	If there is a power failure, it will not be detected since the power modules cannot be polled. The system will continue to report the state of the power modules as they were when last seen.
Recovery	Correct the power shelf controller communications problem.

12.286 tmnxPowerShelfCommsUp

Table 440: tmnxPowerShelfCommsUp properties

Property name	Value
Application name	CHASSIS
Event ID	6003
Event name	tmnxPowerShelfCommsUp
SNMP notification prefix and OID	TIMETRA-POWER-SHELF-MIB.tmnxPowerShelfNotifications.3
Default severity	cleared

Property name	Value
Source stream	main
Message format string	Re-established communications to *$tmnxHwIndex$*
Cause	The tmnxPowerShelfCommsUp notification is generated when a loss of communications with the power shelf controller has been resolved.
Effect	Power failures can be detected.
Recovery	No recovery required.

12.287 tmnxPowerShelfInputPwrModeSwitch

Table 441: tmnxPowerShelfInputPwrModeSwitch properties

Property name	Value
Application name	CHASSIS
Event ID	6001
Event name	tmnxPowerShelfInputPwrModeSwitch
SNMP notification prefix and OID	TIMETRA-POWER-SHELF-MIB.tmnxPowerShelfNotifications.1
Default severity	minor
Source stream	main
Message format string	*$tmnxHwIndex$* input power mode switched to *$tmnxPowerShelfInput PowerMode$*A
Cause	The tmnxPowerShelfInputPwrModeSwitch is generated when tmnx PowerShelfInputPowerMode has changed value.
Effect	No effect.
Recovery	No recovery required.

12.288 tmnxPowerShelfOutputStatusDown

Table 442: tmnxPowerShelfOutputStatusDown properties

Property name	Value
Application name	CHASSIS
Event ID	6005
Event name	tmnxPowerShelfOutputStatusDown
SNMP notification prefix and OID	TIMETRA-POWER-SHELF-MIB.tmnxPowerShelfNotifications.5
Default severity	minor
Source stream	main
Message format string	*$tmnxHwIndex$* output status switched to *$tmnxPowerShelfOutput Status$*
Cause	The tmnxPowerShelfOutputStatusSwitch is generated when the physical output switch on the power shelf is set to Standby.
Effect	The power output from the identified power shelf is switched off and does not supply power to the system.
Recovery	Set output switch to On to restore power output.

12.289 tmnxPowerShelfOutputStatusSwitch

Table 443: tmnxPowerShelfOutputStatusSwitch properties

Property name	Value
Application name	CHASSIS
Event ID	6004
Event name	tmnxPowerShelfOutputStatusSwitch
SNMP notification prefix and OID	TIMETRA-POWER-SHELF-MIB.tmnxPowerShelfNotifications.4
Default severity	minor
Source stream	main
Message format string	*$tmnxHwIndex$* output status switched to *$tmnxPowerShelfOutput Status$*

Property name	Value
Cause	The tmnxPowerShelfOutputStatusSwitch is generated when tmnx PowerShelfOutputStatus has changed value.
Effect	No effect.
Recovery	No recovery required.

12.290 tmnxPowerShelfOutputStatusUp

Table 444: tmnxPowerShelfOutputStatusUp properties

Property name	Value
Application name	CHASSIS
Event ID	6006
Event name	tmnxPowerShelfOutputStatusUp
SNMP notification prefix and OID	TIMETRA-POWER-SHELF-MIB.tmnxPowerShelfNotifications.6
Default severity	minor
Source stream	main
Message format string	*$tmnxHwIndex$* output status switched to *$tmnxPowerShelfOutput Status$*
Cause	The tmnxPowerShelfOutputStatusSwitch is generated when the physical output switch on the power shelf is set to On.
Effect	Power output from the identified power shelf is enabled and now supplies power to the system.
Recovery	No recovery required.

12.291 tmnxPowerSupplyFanFailed

Table 445: tmnxPowerSupplyFanFailed properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	2430
Event name	tmnxPowerSupplyFanFailed
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.295
Default severity	minor
Source stream	main
Message format string	Power supply *$tmnxHwIndex$* fan failed
Cause	The tmnxPowerSupplyFanFailed notification is generated when a fan within a particular power-supply has ceased to function normally.
Effect	Cooling to the power-supply may be reduced, potentially leading to overheating.
Recovery	The power-supply should be replaced by one with fully-functioning fan elements.

12.292 tmnxPowerSupplyFanFailedClear

Table 446: tmnxPowerSupplyFanFailedClear properties

Property name	Value
Application name	CHASSIS
Event ID	2431
Event name	tmnxPowerSupplyFanFailedClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.296
Default severity	minor
Source stream	main
Message format string	Power supply *$tmnxHwIndex$* fan failure cleared
Cause	The tmnxPowerSupplyFanFailedClear notification is generated when the fan component of a power-supply has been restored to normal operation.
Effect	N/A
Recovery	N/A

12.293 tmnxRedPrimaryCPMFail

Table 447: 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
Source stream	main
Message format string	Active CPM failed
Cause	Generated when the primary CPM fails.
Effect	N/A
Recovery	N/A

12.294 tmnxSasAlarminput1StateChanged

Table 448: tmnxSasAlarminput1StateChanged properties

Property name	Value
Application name	CHASSIS
Event ID	3001
Event name	tmnxSasAlarminput1StateChanged
SNMP notification prefix and OID	TIMETRA-SAS-ALARM-INPUT-MIB.tmnxSasAlarmInputNotifications.1
Default severity	major
Source stream	main
Message format string	Alarm Input "*$tmnxSasAlarmInputDescription$*" has changed status "*$tmnxSasAlarmInputNotifyMessage$*"

Property name	Value
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.

12.295 tmnxSasAlarminput2StateChanged

Table 449: 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
Source stream	main
Message format string	Alarm Input "*$tmnxSasAlarmInputDescription$*" has changed status "*$tmnxSasAlarmInputNotifyMessage$*"
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 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

Property name	Value
	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.

12.296 tmnxSasAlarminput3StateChanged

Table 450: 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
Source stream	main
Message format string	Alarm Input "*$tmnxSasAlarmInputDescription$*" has changed status "*$tmnxSasAlarmInputNotifyMessage$*"
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.

12.297 tmnxSasAlarminput4StateChanged

Table 451: 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
Source stream	main
Message format string	Alarm Input "*$tmnxSasAlarmInputDescription$*" has changed status "*$tmnxSasAlarmInputNotifyMessage$*"
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.

12.298 tmnxSfmIcPortDDMClear

Table 452: tmnxSfmIcPortDDMClear properties

Property name	Value
Application name	CHASSIS

Property name	Value
Event ID	4026
Event name	tmnxSfmIcPortDDMClear
SNMP notification prefix and OID	TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmIcPort Notifications.7
Default severity	minor
Source stream	main
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

12.299 tmnxSfmIcPortDDMFailure

Table 453: 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
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	N/A

12.300 tmnxSfmIcPortDegraded

Table 454: 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
Source stream	main
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."

12.301 tmnxSfmIcPortDegradedClear

Table 455: 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
Default severity	minor
Source stream	main
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

12.302 tmnxSfmIcPortDown

Table 456: 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
Source stream	main
Message format string	Possible messages:

Property name	Value
	• 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.
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.

12.303 tmnxSfmIcPortSFFInserted

Table 457: 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
Source stream	main
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

12.304 tmnxSfmIcPortSFFRemoved

Table 458: 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
Source stream	main
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.

12.305 tmnxSfmIcPortUp

Table 459: 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

Property name	Value
Source stream	main
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

12.306 tmnxSyncIfTimBITS2048khzUnsup

Table 460: tmnxSyncIfTimBITS2048khzUnsup properties

Property name	Value
Application name	CHASSIS
Event ID	2134
Event name	tmnxSyncIfTimBITS2048khzUnsup
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.123
Default severity	major
Source stream	main
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)'.

12.307 tmnxSyncIfTimBITS2048khzUnsupClr

Table 461: 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
Source stream	main
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.
Recovery	No recovery required.

12.308 tmnxTunnelGrpEsaVmActivity

Table 462: tmnxTunnelGrpEsaVmActivity properties

Property name	Value
Application name	CHASSIS
Event ID	2208
Event name	tmnxTunnelGrpEsaVmActivity
SNMP notification prefix and OID	TIMETRA-CHASSIS-MIB.tmnxChassisNotification.219

Property name	Value
Default severity	minor
Source stream	main
Message format string	esa-*$tmnxEsaId$*/*$tmnxEsaVmId$* is *$tmnxTunnelGrpEsaVmActive$* in tunnel group *$tmnxTunnelGrpEsaVmGroupAssoc$*
Cause	The tmnxTunnelGrpEsaVmActivity notification is generated when a tunnel-capable ESA virtual machine that is associated with a tunnel group becomes active or inactive within its group.
Effect	N/A
Recovery	N/A

13 DEBUG

13.1 traceEvent

Table 463: traceEvent properties

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

14 DHCP

14.1 sapDHCPLeaseEntriesExceeded

Table 464: 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
Source stream	main
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.

14.2 sapDHCPLseStateMobilityError

Table 465: sapDHCPLseStateMobilityError properties

Property name	Value
Application name	DHCP
Event ID	2027
Event name	sapDHCPLseStateMobilityError
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.22
Default severity	warning
Source stream	main
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.

14.3 sapDHCPLseStateOverride

Table 466: 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
Source stream	main
Message format string	Existing lease state (ipAddr = *$svcDhcpLseStateOldCiAddr$*, macAddr = *$svcDhcpLseStateOldChAddr$*) on SAP *$sapEncapValue$* in service *$svcId$* overridden to (ipAddr = *$svcDhcpLseStateNewCiAddr$*, mac Addr = *$svcDhcpLseStateNewChAddr$*)

Property name	Value
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

14.4 sapDHCPLseStatePopulateErr

Table 467: 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
Source stream	main
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.

14.5 sapDHCPProxyServerError

Table 468: 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
Source stream	main
Message format string	DHCP Proxy error on SAP *$sapEncapValue$* in service *$svcId$* - *$svcDhcpProxyError$*
Cause	The sapDHCPProxyServerError notification indicates that the system was unable to proxy DHCP requests.
Effect	N/A
Recovery	Contact Nokia customer service.

14.6 sapDHCPSuspiciousPcktRcvd

Table 469: 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
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	Contact Nokia customer service.

14.7 sapStatHost6DynMacConflict

Table 470: 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
Source stream	main
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.
Recovery	The recovery action depends on the exact reason why the MAC update failed. This is clarified in the sapNotifyReason object.

14.8 sapStaticHostDynMacConflict

Table 471: sapStaticHostDynMacConflict properties

Property name	Value
Application name	DHCP
Event ID	2012

Property name	Value
Event name	sapStaticHostDynMacConflict
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.16
Default severity	warning
Source stream	main
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.

14.9 sdpBindDHCPLeaseEntriesExceeded

Table 472: 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
Source stream	main
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.

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

14.10 sdpBindDHCPLseStateMobilityErr

Table 473: 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
Source stream	main
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.

14.11 sdpBindDHCPLseStateOverride

Table 474: sdpBindDHCPLseStateOverride properties

Property name	Value
Application name	DHCP
Event ID	2007
Event name	sdpBindDHCPLseStateOverride

Property name	Value
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.11
Default severity	warning
Source stream	main
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

14.12 sdpBindDHCPLseStatePopulateErr

Table 475: 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
Source stream	main
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.

Property name	Value
Recovery	Contact Nokia customer service.

14.13 sdpBindDHCPProxyServerError

Table 476: 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
Source stream	main
Message format string	DHCP Proxy error on SDP Bind *$sdpBindId$* in service *$svcId$* - *$svc DhcpProxyError$*
Cause	The sdpBindDHCPProxyServerError notification indicates that the system was unable to proxy DHCP requests.
Effect	N/A
Recovery	Contact Nokia customer service.

14.14 sdpBindDHCPSuspiciousPcktRcvd

Table 477: sdpBindDHCPSuspiciousPcktRcvd properties

Property name	Value
Application name	DHCP
Event ID	2008
Event name	sdpBindDHCPSuspiciousPcktRcvd
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.12

Property name	Value
Default severity	warning
Source stream	main
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
Recovery	Contact Nokia customer service.

14.15 svcDHCPLseStateRestoreProblem

Table 478: 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
Source stream	main
Message format string	Problem occurred 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.

14.16 svcDHCPMiscellaneousProblem

Table 479: 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
Source stream	main
Message format string	*$tmnxFailureDescription$*
Cause	The svcDHCPMiscellaneousProblem notification is generated on miscellaneous DHCP problems.
Effect	N/A
Recovery	Contact Nokia customer service.

14.17 tmnxVRtrDHCP6AssignedIllegSubnet

Table 480: 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
Source stream	main
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 *$vRtrID$*)

Property name	Value
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.

14.18 tmnxVRtrDHCP6ClientMacUnresolved

Table 481: tmnxVRtrDHCP6ClientMacUnresolved properties

Property name	Value
Application name	DHCP
Event ID	2026
Event name	tmnxVRtrDHCP6ClientMacUnresolved
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.27
Default severity	warning
Source stream	main
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.

14.19 tmnxVRtrDHCP6IllegalClientAddr

Table 482: 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
Source stream	main
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.

14.20 tmnxVRtrDHCP6LseStateOverride

Table 483: 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
Source stream	main
Message format string	Override existing lease state (inetAddr = *$vRtrDHCP6OldAssignedNetAddr$*/ *$vRtrDHCP6OldAssignedPrefixLen$*, chAddr = *$vRtrDhcpLseStateOldChAddr$*, DUID = *$vRtrDHCP6OldClientId$*) on interface *$v*

Property name	Value
	RtrIfName$* in service *$vRtrServiceId$* (vRtr *$vRtrID$*) to (inetAddr = *$vRtrDHCP6AssignedNetAddr$/ $vRtrDHCP6AssignedPrefixLen$, chAddr = *$vRtrDhcpLseStateNewChAddr$*, DUID = *$vRtrDHCP6New ClientId$*) - *$vRtrDHCP6LeaseOverrideResult$*
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

14.21 tmnxVRtrDHCP6RelayLseStExceeded

Table 484: 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
Source stream	main
Message format string	Lease state for (inetAddr = *$vRtrDHCP6AssignedNetAddr$*/*$v RtrDHCP6AssignedPrefixLen$*, DUID = *$vRtrDHCP6NewClientId $*, leaseTime = *$svcDhcpClientLease$*) was not stored because the number of DHCP6 relay lease states on interface *$vRtrIfName$* in service *$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.

14.22 tmnxVRtrDHCP6RelayReplyStripUni

Table 485: 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
Source stream	main
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

14.23 tmnxVRtrDHCP6ServerLseStExceeded

Table 486: tmnxVRtrDHCP6ServerLseStExceeded properties

Property name	Value
Application name	DHCP
Event ID	2021
Event name	tmnxVRtrDHCP6ServerLseStExceeded
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.22
Default severity	warning

Property name	Value
Source stream	main
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.

14.24 tmnxVRtrDHCPIfLseStatesExceeded

Table 487: 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
Source stream	main
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.
Effect	N/A

Property name	Value
Recovery	Investigate the cause of the excessive DHCP lease states.

14.25 tmnxVRtrDHCPSuspiciousPcktRcvd

Table 488: 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
Source stream	main
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.

15 DHCPS

15.1 tmnxDhcpsAddrAllocationFailure

Table 489: 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
Source stream	main
Message format string	Server "*$tmnxDhcpSvrNotifServerName$*" could not allocate IP address to client (mac= *$tmnxDhcpSvrNotifMsgHwAddress$* gi-addr= *$tmnxDhcpSvrNotifGatewayIpAddr$* pri-pool="*$tmnxDhcpSvrNotif PrimaryPool$*" sec-pool=" *$tmnxDhcpSvrNotifSecondaryPool$*"). 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.

15.2 tmnxDhcpsFoLeaseUpdateFailed

Table 490: 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
Default severity	warning
Source stream	main
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.

15.3 tmnxDhcpsFoStateChange

Table 491: 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
Source stream	main
Message format string	DHCP server *$tmnxDhcpServerCfgServerName$* changed failover state: *$tmnxDhcpsFoState$*.
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.

15.4 tmnxDhcpsLeaseOfferedExpired

Table 492: tmnxDhcpsLeaseOfferedExpired properties

Property name	Value
Application name	DHCPS
Event ID	2034

Property name	Value
Event name	tmnxDhcpsLeaseOfferedExpired
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.34
Default severity	warning
Source stream	main
Message format string	Lease offered by server "*$tmnxDhcpServerCfgServerName$*" ip-address " *$tmnxDhcpSvrLeaseClientAddress$*" to client (mac=*$tmnxDhcpSvrNotifMsgHwAddress$* 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.
Recovery	The recovery action, if any, will depend on the reason of the expiry.

15.5 tmnxDhcpsPacketDropped

Table 493: 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
Source stream	main
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.

Property name	Value
Effect	Some client request fails. The client will have to try again.
Recovery	The recovery action, if any, will depend on the reason.

15.6 tmnxDhcpsPoolFoLeaseUpdateFailed

Table 494: 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
Source stream	main
Message format string	BNDUPD message could not be processed for DHCP lease (server Name= *$tmnxDhcpServerCfgServerName$*, pool=*$tmnxDhcpServer PoolName$*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

15.7 tmnxDhcpsPoolFoStateChange

Table 495: tmnxDhcpsPoolFoStateChange properties

Property name	Value
Application name	DHCPS
Event ID	2024
Event name	tmnxDhcpsPoolFoStateChange
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.24
Default severity	warning
Source stream	main
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

15.8 tmnxDhcpSvrDeclineStaticAddr

Table 496: 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
Source stream	main
Message format string	DHCP static IP address (serverName=*$tmnxDhcpSvrNotifServerName $*, ipAddr= *$tmnxDhcpSvrNotifLeaseClientAddr$*) is declined by client (HwAddr=*$tmnxDhcpSvrNotifMsgHwAddress$*)

Property name	Value
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.

15.9 tmnxDhcpSvrHostConflict

Table 497: 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
Source stream	main
Message format string	DHCP server *$tmnxDhcpSvrNotifServerName$* detects IP address assignment conflict for host (name= *$tmnxDhcpSvrNotifHostName $*, type=*$tmnxDhcpSvrNotifHostType$*) sender (mac=*$tmnxDhcpSvr NotifMsgHwAddress$*); ipAddr= *$tmnxDhcpSvrNotifLeaseClientAddr$*. *$tmnxDhcpSvrNotifDescription$*
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.

15.10 tmnxDhcpSvrIntLseConflict

Table 498: 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
Source stream	main
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

15.11 tmnxDhcpSvrLeaseCreate

Table 499: tmnxDhcpSvrLeaseCreate properties

Property name	Value
Application name	DHCPS
Event ID	2018
Event name	tmnxDhcpSvrLeaseCreate

Property name	Value
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.18
Default severity	warning
Source stream	main
Message format string	Lease for server "*$tmnxDhcpServerCfgServerName$*" ip-address " *$tmnxDhcpSvrLeaseClientAddress$*" client (mac=*$tmnxDhcpSvr NotifMsgHwAddress$* 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

15.12 tmnxDhcpSvrLeaseDefaultTimers

Table 500: 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
Source stream	main
Message format string	Reverted to default lease timers for DHCP lease (serverName= *$tmnx DhcpSvrNotifServerName$*, ipAddr=*$tmnxDhcpSvrNotifLeaseClient Addr$*) client (mac=*$tmnxDhcpSvrNotifMsgHwAddress$* DUID=0x *$tmnxDhcpSvrNotifClientDUID$*)-- *$tmnxDhcpSvrNotifDescription$*
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.

Property name	Value
	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

15.13 tmnxDhcpSvrLeaseDelete

Table 501: 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
Source stream	main
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

15.14 tmnxDhcpSvrLeaseModify

Table 502: 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
Source stream	main
Message format string	Lease for server "*$tmnxDhcpServerCfgServerName$*" ip-address " *$tmnxDhcpSvrLeaseClientAddress$*" client (mac=*$tmnxDhcpSvr NotifMsgHwAddress$* 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

15.15 tmnxDhcpSvrLeaseNotOwner

Table 503: 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
Source stream	main
Message format string	DHCP lease (serverName=*$tmnxDhcpSvrNotifServerName$*, ipAddr= *$tmnxDhcpSvrNotifLeaseClientAddr$*, ipAddrLen=*$tmnxDhcpSvrNotif*

Property name	Value
	LeaseClientAddrLen$*) is not owned by sender of DHCP message (Hw Addr= *$tmnxDhcpSvrNotifMsgHwAddress$*, DUID=0x*$tmnxDhcpSvr NotifClientDUID$*) *$tmnxDhcpSvrNotifDescription$
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.

15.16 tmnxDhcpSvrMaxLeasesReached

Table 504: 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
Source stream	main
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.

15.17 tmnxDhcpSvrMsgTooLong

Table 505: tmnxDhcpSvrMsgTooLong properties

Property name	Value
Application name	DHCPS
Event ID	2006
Event name	tmnxDhcpSvrMsgTooLong
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.6
Default severity	warning
Source stream	main
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'.

15.18 tmnxDhcpSvrNoContFreeBlocks

Table 506: tmnxDhcpSvrNoContFreeBlocks properties

Property name	Value
Application name	DHCPS
Event ID	2022

Property name	Value
Event name	tmnxDhcpSvrNoContFreeBlocks
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.20
Default severity	warning
Source stream	main
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 only generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv6(2)'. More detailed information about the failure is indicated in the tmnxDhcpSvrNotifString object.
Effect	N/A
Recovery	N/A

15.19 tmnxDhcpSvrNoSubnetFixAddr

Table 507: 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
Source stream	main
Message format string	DHCP server *$tmnxDhcpSvrNotifServerName$* could not find subnet for fixed IP address *$tmnxDhcpSvrNotifLeaseClientAddr$* of host (db name =*$tmnxDhcpSvrNotifUserDatabaseName$*, host name= *$tmnxDhcpSvrNotifHostName$*, type=*$tmnxDhcpSvrNotifHostType$*) --

Property name	Value
	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.

15.20 tmnxDhcpSvrPfxThDepletedV6

Table 508: 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
Source stream	main
Message format string	No free prefixes with minimum threshold length *$tmnxDhcpsPfxMin FreePrefixLen$* in prefix ' *$tmnxDhcpSvrSubnetAddress$*/*$tmnxDhcp SvrSubnetPrefixLength$*' in pool '*$tmnxDhcpServerPoolName$*' 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.

Property name	Value
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.

15.21 tmnxDhcpSvrPfxThTooLowV6

Table 509: 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
Source stream	main
Message format string	The number of prefixes with minimum threshold length *$tmnxDhcpsPfxMinFreePrefixLen$* in prefix *$tmnxDhcpSvrSubnetAddress$*/*$tmnxDhcpSvrSubnetPrefixLength$*, pool *$tmnxDhcpServerPoolName$*, server *$tmnxDhcpServerCfgServerName$* is becoming low. *$tmnxDhcpsPfxThCurrFreeBlksHw$*/*$tmnxDhcpsPfxThCurrFreeBlksLw$* free prefix(es). (Minimum free threshold *$tmnxDhcpsPfxMinFreePercent$*%/*$tmnxDhcpsPfxMinFreeNumber$*)
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.

15.22 tmnxDhcpSvrPlThDepletedV6

Table 510: 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
Source stream	main
Message format string	No free prefixes with minimum threshold length *$tmnxDhcpsPlMinFreePrefixLen$* in pool ' *$tmnxDhcpServerPoolName$*' in server '*$tmnxDhcpServerCfgServerName$*'.
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.

15.23 tmnxDhcpSvrPlThTooLowV6

Table 511: 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
Source stream	main

Property name	Value
Message format string	The number of prefixes with minimum threshold length *$tmnxDhcps PfxMinFreePrefixLen$* in pool ' *$tmnxDhcpSvrPoolName$*', server *$tmnxDhcpServerCfgServerName$* is becoming low. *$tmnxDhcpsPlTh CurrFreeBlksHw$*/ *$tmnxDhcpsPlThCurrFreeBlksLw$* 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.

15.24 tmnxDhcpSvrPoolDepleted

Table 512: 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
Source stream	main
Message format string	No free addresses in pool "*$tmnxDhcpServerPoolName$*"
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

15.25 tmnxDhcpSvrPoolMinFreeExc

Table 513: 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
Source stream	main
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.

15.26 tmnxDhcpSvrPoolUnknown

Table 514: tmnxDhcpSvrPoolUnknown properties

Property name	Value
Application name	DHCPS
Event ID	2003
Event name	tmnxDhcpSvrPoolUnknown

Property name	Value
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.3
Default severity	warning
Source stream	main
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.

15.27 tmnxDhcpSvrSubnetDepleted

Table 515: 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
Source stream	main
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 only generated for DHCP server instances with the value of tmnxDhcp ServerCfgAddrType set to 'ipv4(1)'.
Effect	N/A

Property name	Value
Recovery	N/A

15.28 tmnxDhcpSvrSubnetMinFreeExc

Table 516: 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
Source stream	main
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.

15.29 tmnxDhcpSvrUserDbUnknown

Table 517: tmnxDhcpSvrUserDbUnknown properties

Property name	Value
Application name	DHCPS
Event ID	2009
Event name	tmnxDhcpSvrUserDbUnknown
SNMP notification prefix and OID	TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.9
Default severity	warning
Source stream	main
Message format string	User database *$tmnxDhcpServerCfgUserDatabase$* specified for server *$tmnxDhcpServerCfgServerName$* does not exist -- dropping DHCP message from sender (mac=*$tmnxDhcpSvrNotifMsgHwAddress$*)
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.

15.30 tmnxLudbDhcpGroupIfTooLong

Table 518: 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

Property name	Value
Source stream	main
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
Recovery	N/A

15.31 tmnxLudbPppoeGroupIfTooLong

Table 519: 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
Source stream	main
Message format string	"*$tmnxLocUsrDbPppoeDefMsapGroupIf$*" concatenated with " *$tmnx LudbNotifyPortId$*" 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

16 DIAMETER

16.1 tmnxDiamAppSessionFailure

Table 520: 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
Source stream	main
Message format string	DIAMETER session failure, sessid= *$tmnxDiamAppSessionId$*, subscrid=*$tmnxDiamAppSubscrId$*, sapid=*$tmnxDiamAppSapId$*, slaprof= *$tmnxDiamAppSLAProfName$ $tmnxDiamNotifySpiShare Type$*:*$tmnxDiamNotifySpiShareId$*, *$tmnxDiamAppTrapDescription$*
Cause	The tmnxDiamAppSessionFailure notification indicates that the DIAMETER protocol has a session failure.
Effect	Determined by cc-failure-handling settings.
Recovery	N/A

16.2 tmnxDiamMessageDropped

Table 521: tmnxDiamMessageDropped properties

Property name	Value
Application name	DIAMETER
Event ID	2007

Property name	Value
Event name	tmnxDiamMessageDropped
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.7
Default severity	minor
Source stream	main
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

16.3 tmnxDiamNdPeerStatActiveChanged

Table 522: tmnxDiamNdPeerStatActiveChanged properties

Property name	Value
Application name	DIAMETER
Event ID	2008
Event name	tmnxDiamNdPeerStatActiveChanged
SNMP notification prefix and OID	TIMETRA-DIAMETER-MIB.tmnxDiameterNotifications.8
Default severity	minor
Source stream	main
Message format string	DIAMETER node *$tmnxDiamNodeOriginHost$*, peer *$tmnxDiamNodeDestinationHost$* is *$tmnxDiamNdPeerStatActive$* active
Cause	The value of tmnxDiamNdPeerStatActive can be impacted by various conditions, such as configuration, routing, physical connectivity, and so on.

Property name	Value
Effect	When the peer is active, the diameter applications can use it. When the peer is not active, the diameter applications can not use the peer; there may be a standby peer available to use.
Recovery	The recovery actions, if any are required, depend on the actual condition that affected the activity of the peer.

16.4 tmnxDiamPolicyPeerStateChange

Table 523: 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
Source stream	main
Message format string	DIAMETER policy *$tmnxDiamPlcyName$*, peer *$tmnxDiamPlcyPeer Name$* now has operational state: PrimarySecondary = *$tmnxDiam PeerPrimarySecondary$*, connectionSuspended = *$tmnxDiamPeer ConnectionSuspended$* and cooldownSeqActive = *$tmnxDiamPeer CooldownSeqActive$*, *$tmnxDiamAppTrapDescription$*
Cause	The state of the diameter policy peer changed.
Effect	N/A
Recovery	No recovery is necessary.

16.5 tmnxDiamPpPrxMcLocStateChanged

Table 524: 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
Source stream	main
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.

16.6 tmnxDiamSessionEvent

Table 525: 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
Source stream	main

Property name	Value
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 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.

17 DOT1X

17.1 alxDot1xHostAuthEvent

Table 526: alxDot1xHostAuthEvent properties

Property name	Value
Application name	DOT1X
Event ID	2001
Event name	alxDot1xHostAuthEvent
SNMP notification prefix and OID	ALCATEL-IEEE8021-PAE-MIB.alxDot1xNotifications.1
Default severity	warning
Source stream	security
Message format string	IEEE 802.1X host *$alxDot1xNotifyMacAddress$* port *$alxDot1xNotifyPort$* authentication *$alxDot1xNotifyAuthHostEvent$$alxDot1xNotifyDescription$*
Cause	A state change occurred while authenticating a host.
Effect	The effect depends on the particular event. If the event is a failure, the value of the object alxDot1xNotifyDescription may contain additional information.
Recovery	Recovery, if any, depends on the particular event.

18 DYNSVC

18.1 tmnxDynSvcSapFailed

Table 527: 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
Source stream	main
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.

19 EFM_OAM

19.1 dot3OamNonThresholdEvent

Table 528: 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
Source stream	main
Message format string	Port *$ifIndex$* raised *$dot3OamEventLogLocation$* fault *$dot3OamEventLogType$*
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

19.2 dot3OamThresholdEvent

Table 529: dot3OamThresholdEvent properties

Property name	Value
Application name	EFM_OAM
Event ID	2004
Event name	dot3OamThresholdEvent
SNMP notification prefix and OID	DOT3-OAM-MIB.dot3OamNotifications.1
Default severity	major
Source stream	main
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

19.3 tmnxDot3OamLoopCleared

Table 530: 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

Property name	Value
Default severity	minor
Source stream	main
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
Recovery	N/A

19.4 tmnxDot3OamLoopDetected

Table 531: 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
Source stream	main
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

19.5 tmnxDot3OamNonThresholdEventClr

Table 532: 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
Source stream	main
Message format string	Port *$ifIndex$* cleared *$dot3OamEventLogLocation$* fault *$dot3OamEventLogType$*
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.

19.6 tmnxDot3OamPeerChanged

Table 533: 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
Source stream	main
Message format string	Peer MAC for port *$subject$* has changed to *$dot3OamPeerMacAddress$*

Property name	Value
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

19.7 tmnxDot3OamSdThresholdEvent

Table 534: tmnxDot3OamSdThresholdEvent properties

Property name	Value
Application name	EFM_OAM
Event ID	2006
Event name	tmnxDot3OamSdThresholdEvent
SNMP notification prefix and OID	TIMETRA-DOT3-OAM-MIB.tmnxDot3OamNotifications.4
Default severity	minor
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	N/A

19.8 tmnxDot3OamThresholdEventClr

Table 535: 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
Source stream	main
Message format string	Port *$ifIndex$* cleared *$dot3OamEventLogLocation$* SF fault *$dot3OamEventLogType$* - *$dot3OamEventLogValue$* errors 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.

20 ELMI

20.1 tmnxElmiEVCStatusChangeEvent

Table 536: 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
Source stream	main
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

20.2 tmnxElmiIfStatusChangeEvent

Table 537: tmnxElmiIfStatusChangeEvent properties

Property name	Value
Application name	ELMI
Event ID	2001

Property name	Value
Event name	tmnxElmiIfStatusChangeEvent
SNMP notification prefix and OID	TIMETRA-ELMI-MIB.tmnxElmiNotifications.1
Default severity	minor
Source stream	main
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.

21 ERING

21.1 tmnxEthRingApsPrvsnClearAlarm

Table 538: 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
Source stream	main
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

21.2 tmnxEthRingApsPrvsnRaiseAlarm

Table 539: tmnxEthRingApsPrvsnRaiseAlarm properties

Property name	Value
Application name	ERING
Event ID	2002
Event name	tmnxEthRingApsPrvsnRaiseAlarm

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

21.3 tmnxEthRingPathFwdStateChange

Table 540: 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
Source stream	main
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.

22 ETH_CFM

22.1 dot1agCfmFaultAlarm

Table 541: 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
Source stream	main
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

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

22.2 tmnxDot1agCfmMepAisStateChanged

Table 542: 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
Source stream	main
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

22.3 tmnxDot1agCfmMepCsfStateChanged

Table 543: 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

Property name	Value
Default severity	minor
Source stream	main
Message format string	Possible messages: • MEP *$dot1agCfmMdIndex$*/*$dot1agCfmMaIndex$*/ *$dot1agCfmMepIdentifier$* is clear of CSF state • MEP *$dot1agCfmMdIndex$*/*$dot1agCfmMaIndex$*/ *$dot1agCfmMepIdentifier$* is in CSF state
Cause	The tmnxDot1agCfmMepCsfStateChanged notification is generated when a MEP enters or exits a CSF state.
Effect	N/A
Recovery	N/A

22.4 tmnxDot1agCfmMepDMTestComplete

Table 544: 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
Source stream	main
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

22.5 tmnxDot1agCfmMepEthTestComplete

Table 545: 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
Default severity	minor
Source stream	main
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

22.6 tmnxDot1agCfmMepFcltyFaultClear

Table 546: tmnxDot1agCfmMepFcltyFaultClear properties

Property name	Value
Application name	ETH_CFM
Event ID	2011

Property name	Value
Event name	tmnxDot1agCfmMepFcltyFaultClear
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.10
Default severity	warning
Source stream	main
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

22.7 tmnxDot1agCfmMepFcltyFaultRaise

Table 547: 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
Source stream	main
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.

Property name	Value
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.

22.8 tmnxDot1agCfmMepLbmTestComplete

Table 548: 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
Source stream	main
Message format string	loopback test results on MEP *$dot1agCfmMdIndex$*/*$dot1agCfmMaIndex$*/ *$dot1agCfmMepIdentifier$* for *$dot1agCfmMepTransmitLbmDestMacAddress$* are available (MEP admin-name = " *$tmnxDot1agCfmMdAdminName$*"/"*$tmnxDot1agCfmMaNetAdminName$*"/*$dot1agCfmMepIdentifier$*)
Cause	The tmnxDot1agCfmMepLbmTestComplete notification indicates that a loopback test has been issued and results are ready.
Effect	N/A
Recovery	N/A

22.9 tmnxDot1agCfmMepLtmTestComplete

Table 549: 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
Source stream	main
Message format string	linktrace test results with sequenceNumber *$dot1agCfmMepTransmitLtmSeqNumber$* on MEP *$dot1agCfmMdIndex$*/*$dot1agCfmMaIndex$*/*$dot1agCfmMepIdentifier$* are now available (MEP admin-name = " *$tmnxDot1agCfmMdAdminName$*"/"*$tmnxDot1agCfmMaNetAdminName$*"/*$dot1agCfmMepIdentifier$*)
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

22.10 tmnxDot1agCfmMepOperGrpStateChgd

Table 550: tmnxDot1agCfmMepOperGrpStateChgd properties

Property name	Value
Application name	ETH_CFM
Event ID	2012
Event name	tmnxDot1agCfmMepOperGrpStateChgd
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.11
Default severity	minor
Source stream	main

Property name	Value
Message format string	Oper-group *$tmnxDot1agCfmMepMonitorOperGrp$* changed MEP *$dot1agCfmMdIndex$*/ *$dot1agCfmMaIndex$*/*$dot1agCfmMep Identifier$* state to *$tmnxDot1agCfmMepOperGrpState$*
Cause	The tmnxDot1agCfmMepOperGrpStateChgd notification is generated when there is a change in the value of tmnxDot1agCfmMepOperGrp State.
Effect	Status of one or more of the members of the operational group has changed to cause the change in operational status of the MEP.
Recovery	Operational status of the members of the operational-group will need to be investigated.

22.11 tmnxDot1agCfmMepSLMTestComplete

Table 551: tmnxDot1agCfmMepSLMTestComplete properties

Property name	Value
Application name	ETH_CFM
Event ID	2008
Event name	tmnxDot1agCfmMepSLMTestComplete
SNMP notification prefix and OID	TIMETRA-IEEE8021-CFM-MIB.tmnxDot1agNotifications.7
Default severity	minor
Source stream	main
Message format string	SLM *$tmnxDot1agCfmMepSlmTestType$* (test-id *$tmnxDot1agCfm MepSlmTestId$*) completed for remote-mep *$tmnxDot1agCfmMepSlm RemoteMepId$* remote MAC *$tmnxDot1agCfmMepSlmRemoteMac Addr$*
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, tmnxDot1agCfmMepSlm PacketLossOut and tmnxDot1agCfmMepSlmPacketUnack values are fixed at 'zero(0)'.
Effect	N/A
Recovery	N/A

22.12 tmnxDot1agCfmMipEvaluation

Table 552: 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
Source stream	main
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

23 ETH_TUNNEL

23.1 tmnxEthTunnelApsCfgClearAlarm

Table 553: tmnxEthTunnelApsCfgClearAlarm properties

Property name	Value
Application name	ETH_TUNNEL
Event ID	2002
Event name	tmnxEthTunnelApsCfgClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.2
Default severity	minor
Source stream	main
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

23.2 tmnxEthTunnelApsCfgRaiseAlarm

Table 554: tmnxEthTunnelApsCfgRaiseAlarm properties

Property name	Value
Application name	ETH_TUNNEL
Event ID	2001
Event name	tmnxEthTunnelApsCfgRaiseAlarm

Property name	Value
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.1
Default severity	minor
Source stream	main
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.

23.3 tmnxEthTunnelApsNoRspClearAlarm

Table 555: tmnxEthTunnelApsNoRspClearAlarm properties

Property name	Value
Application name	ETH_TUNNEL
Event ID	2006
Event name	tmnxEthTunnelApsNoRspClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.6
Default severity	minor
Source stream	main
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

23.4 tmnxEthTunnelApsNoRspRaiseAlarm

Table 556: tmnxEthTunnelApsNoRspRaiseAlarm properties

Property name	Value
Application name	ETH_TUNNEL
Event ID	2005
Event name	tmnxEthTunnelApsNoRspRaiseAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.5
Default severity	minor
Source stream	main
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.

23.5 tmnxEthTunnelApsPrvsnClearAlarm

Table 557: tmnxEthTunnelApsPrvsnClearAlarm properties

Property name	Value
Application name	ETH_TUNNEL
Event ID	2004
Event name	tmnxEthTunnelApsPrvsnClearAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.4
Default severity	minor

Property name	Value
Source stream	main
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

23.6 tmnxEthTunnelApsPrvsnRaiseAlarm

Table 558: tmnxEthTunnelApsPrvsnRaiseAlarm properties

Property name	Value
Application name	ETH_TUNNEL
Event ID	2003
Event name	tmnxEthTunnelApsPrvsnRaiseAlarm
SNMP notification prefix and OID	TIMETRA-ETH-TUNNEL-MIB.tmnxEthTunnelApsNotifications.3
Default severity	minor
Source stream	main
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.

23.7 tmnxEthTunnelApsSwitchoverAlarm

Table 559: tmnxEthTunnelApsSwitchoverAlarm properties

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

24 FILTER

24.1 tFilterApplyPathProblem

Table 560: 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
Source stream	main
Message format string	Problem in *$tFltrPrefixListType$* prefix-list *$tFltrPrefixListName$* for apply-path *$tFltrApplyPathSource$ $tFltrApplyPathIndex$*: *$tFilter AlarmDescription$*
Cause	Failed to add prefix/prefixes specified by the apply-path rule to the prefix list likely due to insufficient resources.
Effect	Prefix list does not contain all prefixes specified by the apply-path rule.
Recovery	Release resources by removing unnecessary prefixes or specify more specific apply-path rule.

24.2 tFilterBgpFlowSpecProblem

Table 561: tFilterBgpFlowSpecProblem properties

Property name	Value
Application name	FILTER
Event ID	2007

Property name	Value
Event name	tFilterBgpFlowSpecProblem
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.7
Default severity	minor
Source stream	main
Message format string	N/A
Cause	N/A
Effect	N/A
Recovery	N/A

24.3 tFilterEmbeddingOperStateChange

Table 562: 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
Source stream	main
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

Property name	Value
	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.

24.4 tFilterEmbedFlowspecOperStateChg

Table 563: 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
Source stream	main
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.

Property name	Value
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.

24.5 tFilterEmbedOpenflowOperStateChg

Table 564: tFilterEmbedOpenflowOperStateChg properties

Property name	Value
Application name	FILTER
Event ID	2012
Event name	tFilterEmbedOpenflowOperStateChg
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.12
Default severity	minor
Source stream	main
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.

24.6 tFilterOpenflowRequestRejected

Table 565: tFilterOpenflowRequestRejected properties

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

24.7 tFilterRadSharedFltrAlarmClear

Table 566: 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
Source stream	main

Property name	Value
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.

24.8 tFilterRadSharedFltrAlarmRaised

Table 567: 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
Source stream	main
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 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 reconsidered.

24.9 tFilterRPActiveDestChangeEvent

Table 568: tFilterRPActiveDestChangeEvent properties

Property name	Value
Application name	FILTER
Event ID	2017
Event name	tFilterRPActiveDestChangeEvent
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.16
Default severity	minor
Source stream	main
Message format string	The active destination of redirect policy *$tFilterRedirectPolicy$* has changed to *$tFilterRPActiveDestAddr$*.
Cause	This notification was triggered because active destination of a redirect policy has changed.
Effect	Traffic hitting filter entries with forward redirect-policy set to this redirect policy will be directed toward the new active destination.
Recovery	No recovery action is required.

24.10 tFilterSubInsFltrEntryDropped

Table 569: 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
Source stream	main

Property name	Value
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.

24.11 tFilterSubInsSpaceAlarmCleared

Table 570: tFilterSubInsSpaceAlarmCleared properties

Property name	Value
Application name	FILTER
Event ID	2005
Event name	tFilterSubInsSpaceAlarmCleared
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.5
Default severity	warning
Source stream	main
Message format string	The range of entries reserved in *$tFilterType$ $tFilterId$* for *$tFilterSub InsSpaceOwner$* has fallen below its configured low watermark level *$t FilterThresholdReached$*
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.

24.12 tFilterSubInsSpaceAlarmRaised

Table 571: 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
Source stream	main
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.

24.13 tIPFilterPBRPacketsDrop

Table 572: 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
Source stream	main

Property name	Value
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/ 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.

25 GSMP

25.1 tmnxAncpEgrRateMonitorEvent

Table 573: 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
Source stream	main
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 subscriber gets less BW than what is currently configured in the system.
Recovery	No recovery is necessary.

25.2 tmnxAncpEgrRateMonitorEventL

Table 574: tmnxAncpEgrRateMonitorEventL properties

Property name	Value
Application name	GSMP

Property name	Value
Event ID	2004
Event name	tmnxAncpEgrRateMonitorEventL
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
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 subscriber gets less BW than what is currently configured in the system.
Recovery	No recovery is necessary.

25.3 tmnxAncpIngRateMonitorEvent

Table 575: 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
Source stream	main
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 *$tmnxNotifAncpPolicyName$*

Property name	Value
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 subscriber gets less BW then what is currently configured in the system.
Recovery	No recovery is necessary.

25.4 tmnxAncpIngRateMonitorEventL

Table 576: tmnxAncpIngRateMonitorEventL properties

Property name	Value
Application name	GSMP
Event ID	2002
Event name	tmnxAncpIngRateMonitorEventL
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
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 subscriber gets less BW than what is currently configured in the system.
Recovery	No recovery is necessary.

25.5 tmnxAncpSesRejected

Table 577: 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
Source stream	main
Message format string	An incoming ANCP session has been rejected: *$tmnxAncpReject Reason$*
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.

25.6 tmnxAncpShcvDisabledEvent

Table 578: 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
Source stream	main
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: *$tmnxNotifAncpPolicyName$*

Property name	Value
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.

25.7 tmnxAncpShcvDisabledEventL

Table 579: tmnxAncpShcvDisabledEventL properties

Property name	Value
Application name	GSMP
Event ID	2006
Event name	tmnxAncpShcvDisabledEventL
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
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.

25.8 tmnxAncpStringRejected

Table 580: 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
Source stream	main
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.

26 IGMP

26.1 vRtrIgmpGrpIfSapCModeRxQueryMism

Table 581: 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
Source stream	main
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

26.2 vRtrIgmpGrpIfSapMaxGrpsLimExceed

Table 582: vRtrIgmpGrpIfSapMaxGrpsLimExceed properties

Property name	Value
Application name	IGMP
Event ID	2012
Event name	vRtrIgmpGrpIfSapMaxGrpsLimExceed
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.12
Default severity	minor
Source stream	main
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

26.3 vRtrIgmpGrpIfSapMaxGrpSrcLimExcd

Table 583: 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
Source stream	main

Property name	Value
Message format string	The number of groups or sources for SAP *$sapPortId$* on interface *$vRtrGrpIfIndex$*, 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
Recovery	N/A

26.4 vRtrIgmpGrpIfSapMaxSrcsLimExceed

Table 584: 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
Source stream	main
Message format string	The number of sources for SAP *$sapPortId$* on interface *$vRtrGrpIfIndex$*, 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

26.5 vRtrIgmpGrpIfSapMcacPlcyDropped

Table 585: 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
Source stream	main
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

26.6 vRtrIgmpGrpIfSapRxQueryVerMism

Table 586: 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

Property name	Value
Source stream	main
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

26.7 vRtrIgmpHostCModeRxQueryMismatch

Table 587: 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
Source stream	main
Message format string	Mismatch between Host compatible mode and the version of the IGMP query received
Cause	N/A
Effect	N/A
Recovery	N/A

26.8 vRtrIgmpHostInstantiationFail

Table 588: 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
Source stream	main
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.

26.9 vRtrIgmpHostMaxGrpsLimitExceeded

Table 589: 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
Source stream	main

Property name	Value
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.

26.10 vRtrIgmpHostMaxGrpSrcsLimitExcd

Table 590: 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
Source stream	main
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 group sources is equal to vRtrIgmpHostMaxGrpSources, the maximum number of group sources per group supported on the host.
Effect	N/A
Recovery	N/A

26.11 vRtrIgmpHostMaxSrcsLimitExceeded

Table 591: 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
Source stream	main
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

26.12 vRtrIgmpHostMcacPlcyDropped

Table 592: vRtrIgmpHostMcacPlcyDropped properties

Property name	Value
Application name	IGMP
Event ID	2007
Event name	vRtrIgmpHostMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.7
Default severity	minor

Property name	Value
Source stream	main
Message format string	IGMP group/source dropped for Subscriber due to MCAC-policy
Cause	N/A
Effect	N/A
Recovery	N/A

26.13 vRtrIgmpHostQryIntervalConflict

Table 593: 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
Source stream	main
Message format string	IGMP-policy query intervals violated for Host on GrpIf in Svc
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

26.14 vRtrIgmpHostRxQueryVerMismatch

Table 594: vRtrIgmpHostRxQueryVerMismatch properties

Property name	Value
Application name	IGMP
Event ID	2009
Event name	vRtrIgmpHostRxQueryVerMismatch
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.9
Default severity	minor
Source stream	main
Message format string	IGMP query received on Host configured as different version
Cause	N/A
Effect	N/A
Recovery	N/A

26.15 vRtrIgmpIfCModeRxQueryMismatch

Table 595: 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
Source stream	main
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 interface.

Property name	Value
Effect	The query will be ignored.
Recovery	No recovery is necessary.

26.16 vRtrIgmpIfRxQueryVerMismatch

Table 596: 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
Source stream	main
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.

26.17 vRtrIgmpMaxGrpsLimitExceeded

Table 597: vRtrIgmpMaxGrpsLimitExceeded properties

Property name	Value
Application name	IGMP
Event ID	2003
Event name	vRtrIgmpMaxGrpsLimitExceeded

Property name	Value
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.3
Default severity	warning
Source stream	main
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.

26.18 vRtrIgmpMaxGrpSrcsLimitExceeded

Table 598: 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
Source stream	main
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

26.19 vRtrIgmpMaxSrcsLimitExceeded

Table 599: 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
Source stream	main
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 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

26.20 vRtrIgmpMcacPlcyDropped

Table 600: 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

Property name	Value
Source stream	main
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.

26.21 vRtrIgmpNotifyNumOfIPsecIfHighWm

Table 601: vRtrIgmpNotifyNumOfIPsecIfHighWm properties

Property name	Value
Application name	IGMP
Event ID	2022
Event name	vRtrIgmpNotifyNumOfIPsecIfHighWm
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.22
Default severity	minor
Source stream	main
Message format string	The number of IPsec multicast interfaces is *$vRtrIgmpNotifyNumOfIPsecIf$* and has almost reached the maximum value *$vRtrIgmpNotifyMaxNumOfIPsecIf$*.
Cause	A vRtrIgmpNotifyNumOfIPsecIfHighWm notification is generated when the number of IPsec interfaces has almost reached the maximum value.
Effect	The system may stop accepting new IPsec multicast interfaces shortly.
Recovery	Use fewer IPsec multicast interfaces.

26.22 vRtrIgmpNotifyNumOfIPsecIfLowWm

Table 602: vRtrIgmpNotifyNumOfIPsecIfLowWm properties

Property name	Value
Application name	IGMP
Event ID	2021
Event name	vRtrIgmpNotifyNumOfIPsecIfLowWm
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.21
Default severity	minor
Source stream	main
Message format string	The number of IPsec multicast interfaces is *$vRtrIgmpNotifyNumOfIPsecIf$* and has dropped back to the low watermark.
Cause	A vRtrIgmpNotifyNumOfIPsecIfLowWm notification is generated when the number of IPsec interfaces has dropped back to the low watermark.
Effect	The system accepts new IPsec multicast interfaces.
Recovery	There is no recovery required for this notification.

26.23 vRtrIgmpNotifyNumOfIPsecIfMaxRch

Table 603: vRtrIgmpNotifyNumOfIPsecIfMaxRch properties

Property name	Value
Application name	IGMP
Event ID	2023
Event name	vRtrIgmpNotifyNumOfIPsecIfMaxRch
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.23
Default severity	minor
Source stream	main

Property name	Value
Message format string	The number of IPsec multicast interfaces has reached its maximum value *$vRtrIgmpNotifyMaxNumOfIPsecIf$*.
Cause	A vRtrIgmpNotifyNumOfIPsecIfMaxRch notification is generated when the number of IPsec interfaces has reached the maximum value.
Effect	The system stops accepting new IPsec multicast interfaces.
Recovery	Delete IPsec multicast interfaces.

26.24 vRtrIgmpSlaProfInstMcacPlcyDrop

Table 604: vRtrIgmpSlaProfInstMcacPlcyDrop properties

Property name	Value
Application name	IGMP
Event ID	2024
Event name	vRtrIgmpSlaProfInstMcacPlcyDrop
SNMP notification prefix and OID	TIMETRA-IGMP-MIB.vRtrIgmpNotifications.24
Default severity	warning
Source stream	main
Message format string	IGMP group/source *$vRtrIgmpNotifyGrpAddr$*/*$vRtrIgmpNotifySrcAddr$* dropped for SLA profile instance subscriber *$tmnxSubIdent$* SAP *$sapNotifyEncapValue$* SLA profile *$tmnxSubNotifSLAProfName$* group *$tmnxSubNotifSpiGroupId$* due to of MCAC policy *$vRtrIgmpNotifyMcacPolicyName$* instance *$vRtrID$*, reason *$vRtrIgmpNotifyDescription$*
Cause	The vRtrIgmpSlaProfInstMcacPlcyDrop event is generated when an IGMP group is dropped on a given SLA profile instance because of applying the multicast CAC policy given by vRtrIgmpNotifyMcacPolicyName.
Effect	The SLA profile instance user cannot receive traffic from the IGMP group.
Recovery	Dropping a multicasts group may be an expected effect of access control; if not, the access control configuration must be modified.

27 IGMP_SNOOPING

27.1 eMplsIgmpSnpgMfibFailure

Table 605: 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
Source stream	main
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

27.2 sapIgmpSnpgGrpLimitExceeded

Table 606: sapIgmpSnpgGrpLimitExceeded properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2001
Event name	sapIgmpSnpgGrpLimitExceeded

Property name	Value
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.1
Default severity	warning
Source stream	main
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.

27.3 sapIgmpSnpgGrpSrcLimitExceeded

Table 607: 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
Source stream	main
Message format string	The number of groups or sources on SAP *$sapEncapValue$* in service *$svcId$* has exceeded the maximum limit of *$sapIgmpSnpgCfgMaxNbrSrcs$* - Dropping source *$alxIgmpSnpgSourceAddress$* for group *$alxIgmpSnpgGroupAddress$*
Cause	The sapIgmpSnpgGrpSrcLimitExceeded notification is generated when an IGMP group or source is dropped on a given SAP because a user configurable upper limit given by sapIgmpSnpgCfgMaxNbrGrpSrcs is reached.
Effect	The specified S,G was not added.

Property name	Value
Recovery	Investigate the cause of the excessive sources.

27.4 sapIgmpSnpgMcacPlcyDropped

Table 608: 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
Source stream	main
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.

27.5 sapIgmpSnpgMcsFailure

Table 609: sapIgmpSnpgMcsFailure properties

Property name	Value
Application name	IGMP_SNOOPING
Event ID	2005
Event name	sapIgmpSnpgMcsFailure

Property name	Value
SNMP notification prefix and OID	ALCATEL-IGMP-SNOOPING-MIB.alxIgmpSnpgSapNotifications.3
Default severity	warning
Source stream	main
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.
Effect	Synchronization between chassis has been lost.
Recovery	No recovery is required.

27.6 sapIgmpSnpgSrcLimitExceeded

Table 610: 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.4
Default severity	warning
Source stream	main
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.

27.7 sdpBndIgmpSnpgGrpLimitExceeded

Table 611: 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
Default severity	warning
Source stream	main
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.

27.8 sdpBndIgmpSnpgGrpSrcLimitExceed

Table 612: 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

Property name	Value
Source stream	main
Message format string	The number of groups or sources on SDP Bind *$sdpBindId$* in service *$svcId$* has exceeded the maximum limit of *$sdpBndIgmpSnpgCfgMaxNbrSrcs$* - 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.

27.9 sdpBndIgmpSnpgMcacPlcyDropped

Table 613: 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
Source stream	main
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.

27.10 sdpBndIgmpSnpgSrcLimitExceeded

Table 614: 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.3
Default severity	warning
Source stream	main
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 configurable upper limit given by sdpBndIgmpSnpgCfgMaxNbrSrcs is reached.
Effect	The specified S,G was not added.
Recovery	Investigate the cause of the excessive sources.

28 IP

28.1 clearRTMError

Table 615: clearRTMError properties

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

28.2 fibAddFailed

Table 616: fibAddFailed properties

Property name	Value
Application name	IP
Event ID	2005
Event name	fibAddFailed
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	major
Source stream	main
Message format string	FIB add failed for VRF *$vRtrID$* prefix *$prefix$*
Cause	FIB resources have been exhausted.
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.

28.3 ipAnyDuplicateAddress

Table 617: ipAnyDuplicateAddress properties

Property name	Value
Application name	IP
Event ID	2010
Event name	ipAnyDuplicateAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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.

28.4 ipArpBadInterface

Table 618: ipArpBadInterface properties

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

28.5 ipArpDuplicateIpAddress

Table 619: ipArpDuplicateIpAddress properties

Property name	Value
Application name	IP
Event ID	2008
Event name	ipArpDuplicateIpAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	duplicate IP address *$ipAddress$* with *$macAddress$* on interface *$interface$*
Cause	Another system on the subnet has the same IP address.

Property name	Value
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.

28.6 ipArpDuplicateMacAddress

Table 620: ipArpDuplicateMacAddress properties

Property name	Value
Application name	IP
Event ID	2009
Event name	ipArpDuplicateMacAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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.

28.7 ipArpInfoOverwritten

Table 621: ipArpInfoOverwritten properties

Property name	Value
Application name	IP

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

28.8 ipDuplicateAddress

Table 622: ipDuplicateAddress properties

Property name	Value
Application name	IP
Event ID	2003
Event name	ipDuplicateAddress
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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.

28.9 ipEtherBroadcast

Table 623: ipEtherBroadcast properties

Property name	Value
Application name	IP
Event ID	2002
Event name	ipEtherBroadcast
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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.
Recovery	Further investigation required on the host.

28.10 labelIndexAllocFailed

Table 624: labelIndexAllocFailed properties

Property name	Value
Application name	IP
Event ID	2011
Event name	labelIndexAllocFailed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main

Property name	Value
Message format string	Failed to allocate index for route label (VRF *$vRtrID$*, prefix *$prefix$*, owner *$routeOwner$*)
Cause	Too many labelled routes in use (beyond platform scale).
Effect	Traffic forwarding will fail for some subset of labelled routes.
Recovery	Use as many or fewer labelled routes as supported by the platform.

28.11 qosNetworkPolicyMallocFailed

Table 625: qosNetworkPolicyMallocFailed properties

Property name	Value
Application name	IP
Event ID	2006
Event name	qosNetworkPolicyMallocFailed
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	main
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.

29 IPSEC

29.1 tIPsecBfdIntfSessStateChgd

Table 626: 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
Source stream	main
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.

29.2 tIPsecRadAcctPlcyFailure

Table 627: tIPsecRadAcctPlcyFailure properties

Property name	Value
Application name	IPSEC
Event ID	2004
Event name	tIPsecRadAcctPlcyFailure

Property name	Value
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.4
Default severity	minor
Source stream	main
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 'tIPsecRadAcctPlcyFail Reason', 'tIPsecRadAcctPlcyTable' configuration may need to be changed.

29.3 tIPsecRUSAFailToAddRoute

Table 628: 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
Source stream	main
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.

29.4 tIPsecRuTnlEncapIpMtuTooSmall

Table 629: 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
Source stream	main
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.

29.5 tIPsecRUTnlFailToCreate

Table 630: tIPsecRUTnlFailToCreate properties

Property name	Value
Application name	IPSEC

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

29.6 tIPsecRUTnlRemoved

Table 631: 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
Source stream	main
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.

Property name	Value
Recovery	N/A

29.7 tIPSecTrustAnchorPrfOprChg

Table 632: tIPSecTrustAnchorPrfOprChg properties

Property name	Value
Application name	IPSEC
Event ID	2005
Event name	tIPSecTrustAnchorPrfOprChg
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.5
Default severity	minor
Source stream	main
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.

29.8 tIPsecTunnelEncapIpMtuTooSmall

Table 633: tIPsecTunnelEncapIpMtuTooSmall properties

Property name	Value
Application name	IPSEC
Event ID	2006
Event name	tIPsecTunnelEncapIpMtuTooSmall

Property name	Value
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.6
Default severity	warning
Source stream	main
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.
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.

29.9 tIPsecTunnelProtocolFailed

Table 634: tIPsecTunnelProtocolFailed properties

Property name	Value
Application name	IPSEC
Event ID	2014
Event name	tIPsecTunnelProtocolFailed
SNMP notification prefix and OID	TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.14
Default severity	minor
Source stream	main
Message format string	IPsec tunnel *$tIPsecNotifTunnelIdentifier$* of type *$tIPsecNotifTunnel Type$* had an abnormal protocol event due to *$tIPsecNotifReason$*.

Property name	Value
Cause	A tIPsecTunnelProtocolFailed notification is generated when a whenever there is abnormal event from protocol perspective to the tunnel, which are indicated by tIPsecNotifReason (e.g., tunnel encounters a dpd-timeout, or no-proposal-chosen during rekey, etc).
Effect	These abnormal events don't always necessarily cause the tunnel to change its operational-status or to be removed.
Recovery	Please refer to operational-flags of the tunnel for more information.

29.10 tmnxIPsecGWOperStateChange

Table 635: 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
Source stream	main
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 IPsec 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 'limited (5)', the IPsec gateway is not fully operationally up due to the conditions indicated in tmnxIPsecTunnelOperFlags and can only negotiate limited new IKE sessions.

Property name	Value
Recovery	Please refer to tmnxIPsecGWOperFlags for information on why the gateway is operationally down.

29.11 tmnxIPsecTunnelOperStateChange

Table 636: 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
Source stream	main
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 IPsec 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 'limited (5)', the IPsec tunnel is operationally up but may not be ready to re-establish the connection until the conditions indicated in the tmnxIPsec TunnelOperFlags are cleared.
Recovery	Please refer to tmnxIPsecTunnelOperFlags for information on why the tunnel is operationally down.

29.12 tmnxSecNotifCmptedCertChnChngd

Table 637: 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
Source stream	security
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.

29.13 tmnxSecNotifCmptedCertHashChngd

Table 638: 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
Source stream	security

Property name	Value
Message format string	Hash of certificate chain changed in cert-profile *$tIPsecNotifCertProfileName$* entry *$tIPsecNotifCertProfEntryId$* due to CA profile *$tIPsecNotifCaProfNames$*
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.

29.14 tmnxSecNotifSendChnNotInCmptChn

Table 639: 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
Source stream	security
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.

Property name	Value
Recovery	Replace the send-chain CA profile that is not in the certificate chain with one that is.

30 ISIS

30.1 tmnxIsisAdjacencyChange

Table 640: 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
Source stream	main
Message format string	Adjacency status changed to *$isisISAdjState$* for interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, LSP-id: *$vRtrIsisTrapLSPIDString$*
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.

30.2 tmnxIsisAdjBfdSessionSetupFail

Table 641: tmnxIsisAdjBfdSessionSetupFail properties

Property name	Value
Application name	ISIS
Event ID	2062

Property name	Value
Event name	tmnxIsisAdjBfdSessionSetupFail
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.34
Default severity	warning
Source stream	main
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.

30.3 tmnxIsisAdjRestartStatusChange

Table 642: 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
Source stream	main
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 adjacency's graceful restart status changes. The tmnxIsisISAdjRestart Status is the new graceful restart state of the adjacency.
Effect	No effect.

Property name	Value
Recovery	No recovery is necessary.

30.4 tmnxIsisAreaMismatch

Table 643: 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
Source stream	main
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.

30.5 tmnxIsisAuthFail

Table 644: 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
Source stream	main
Message format string	Authentication failure on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, fragment: *$vRtrIsisPDUFragmentString$*
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.

30.6 tmnxIsisAutTypeFail

Table 645: 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
Source stream	main

Property name	Value
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.

30.7 tmnxIsisCircIdExhausted

Table 646: 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
Source stream	main
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.

30.8 tmnxIsisCircMtuTooLow

Table 647: tmnxIsisCircMtuTooLow properties

Property name	Value
Application name	ISIS
Event ID	2064
Event name	tmnxIsisCircMtuTooLow
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.36
Default severity	warning
Source stream	main
Message format string	MTU size too low for interface: *$vRtrIfIndex$* (level *$tmnxIsisNotifSystemLevel$*): *$tmnxIsisNotifCircMtuSize$* smaller than *$tmnxIsisNotifCircMinReqMtuSize$* (min required MTU size to transmit LSP or SNP)
Cause	The tmnxIsisCircMtuTooLow notification is sent when we attempt to a) configure a circuit which cannot propagate an LSP or SNP with max size tmnxIsisLevelLSPBuffSize. b) configure tmnxIsisLevelLSPBuffSize which is bigger than tmnxIsisLevelMaxOperLSPBuffSize. c) configure tmnxIsisSysOrigL1LSPBuffSize or tmnxIsisSysOrigL2LSPBuffSize which is bigger than tmnxIsisLevelMaxOperLSPBuffSize.
Effect	No effect.
Recovery	Increase port-mtu or decrease lsp-mtu.

30.9 tmnxIsisCorruptedLSPDetected

Table 648: tmnxIsisCorruptedLSPDetected properties

Property name	Value
Application name	ISIS
Event ID	2031
Event name	tmnxIsisCorruptedLSPDetected

Property name	Value
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.3
Default severity	warning
Source stream	main
Message format string	Corrupted LSP detected on interface: *$vRtrIfIndex$*, level: *$tmnxIsis NotifSystemLevel$*, 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 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.

30.10 tmnxIsisCorruptRemainingLifetime

Table 649: tmnxIsisCorruptRemainingLifetime properties

Property name	Value
Application name	ISIS
Event ID	2066
Event name	tmnxIsisCorruptRemainingLifetime
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.38
Default severity	warning
Source stream	main
Message format string	Possible corrupt Remaining Lifetime *$tmnxIsisLSPLifetimeRemain$* received on LSP *$tmnxIsisLSPIdString$*, for level: *$tmnxIsisLevel$*
Cause	The tmnxIsisCorruptRemainingLifetime notification is sent when an LSP is received with a possible corrupt Remaining Lifetime field. The Remaining Lifetime of a received LSP is considered as possible corrupt based on following algorithm: - The LSP has passed all acceptance tests. - The LSP is newer than the copy in the local LSPDB or no copy present. - The Remaining Lifetime in the received LSP is less than Zero

Property name	Value
	Age Lifetime. - The adjacency to the neighbor from which the LSP is received has been up for a minimum of Zero Age Lifetime.
Effect	It is possible that an LSP is purged prematurely.
Recovery	The ISIS system will try to recover by setting the Remaining Lifetime to the tmnxIsisMinRemainingLspLifetime value.

30.11 tmnxIsisDatabaseOverload

Table 650: 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
Source stream	main
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 unless tmnxIsisNotifyDescription indicates it.

30.12 tmnxIsisExportLimitReached

Table 651: 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
Default severity	major
Source stream	main
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.

30.13 tmnxIsisExportLimitWarning

Table 652: 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
Source stream	main
Message format string	ISIS level *$tmnxIsisNotifSystemLevel$* has reached *$tmnxIsisExport LimitLogPercent$* percent of the export limit *$tmnxIsisExportLimit$*

Property name	Value
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.

30.14 tmnxIsisFailureDisabled

Table 653: 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
Source stream	main
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.

30.15 tmnxIsisFaOperParticipationDown

Table 654: tmnxIsisFaOperParticipationDown properties

Property name	Value
Application name	ISIS
Event ID	2068
Event name	tmnxIsisFaOperParticipationDown
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.40
Default severity	warning
Source stream	main
Message format string	The oper-participation of *$tmnxIsisFlexAlgoId$* in level *$tmnxIsisNotifSystemLevel$* is operationally down due to *$tmnxIsisNotifyDescription$*.
Cause	The tmnxIsisFaOperParticipationDown notification is sent when the Flexible Algorithm Participation is operationally down. This notification occurs each time when: a) there are no Flexible Algorithm Definitions(FADs) present for the Flexible Algorithm. b) the FAD chosen for Flex-Algo calculation has unsupported parameters like unsupported: 1. Metric-Type 2. Calculation-Type 3. Constraint 4. Fad-Flags 5. Sub-Tlv
Effect	The node will cease to participate in that Flexible Algorithm, and won't advertise its participation in SR-algo sub-TLV.
Recovery	The operator may make sure if at least one FAD is present for that Flexible Algorithm, and in case of unsupported FAD, correct the FAD parameters to send supported values from remote side.

30.16 tmnxIsisIDLenMismatch

Table 655: 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

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

30.17 tmnxIsisLdpSyncExit

Table 656: 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
Source stream	main
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.

Property name	Value
Effect	The IGP link metric is restored to normal levels.
Recovery	No recovery is necessary.

30.18 tmnxIsisLdpSyncTimerStarted

Table 657: tmnxIsisLdpSyncTimerStarted properties

Property name	Value
Application name	ISIS
Event ID	2048
Event name	tmnxIsisLdpSyncTimerStarted
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.20
Default severity	warning
Source stream	main
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.

30.19 tmnxIsisLSPPurge

Table 658: tmnxIsisLSPPurge properties

Property name	Value
Application name	ISIS
Event ID	2060
Event name	tmnxIsisLSPPurge

Property name	Value
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.32
Default severity	warning
Source stream	main
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.

30.20 tmnxIsisLSPTooLargeToPropagate

Table 659: 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
Source stream	main
Message format string	LSP too large to propagate - LSP size: *$tmnxIsisNotifLSPSize$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, LSP-id: *$vRtrIsisTrapLSPIDString$*

Property name	Value
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.

30.21 tmnxIsisManualAddressDrops

Table 660: 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
Source stream	main
Message format string	Configured manual area address *$isisManAreaAddrString$* being ignored when computing routes
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.

30.22 tmnxIsisMaxAreaAddrsMismatch

Table 661: 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
Source stream	main
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.

30.23 tmnxIsisMaxSeqExceedAttempt

Table 662: 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
Source stream	main

Property name	Value
Message format string	Protocol disabled due to attempt to exceed the maximum sequence on level: *$tmnxIsisNotifSystemLevel$*, with LSP-id: *$vRtrIsis TrapLSPIDString$*. Shutdown for a while and start over.
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. A possible cause could be that the same system-id is configured on multiple nodes; when 2 nodes have the same system-id they both keep incrementing its LSP sequence number causing the sequence counter to rollover. While the first 6 bytes of the LSPID are ours, the other two contain useful information.
Effect	No effect.
Recovery	No recovery is necessary.

30.24 tmnxIsisOrigLSPBufSizeMismatch

Table 663: 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
Source stream	main
Message format string	Originating LSP buffer size mismatch - LSP size: *$tmnxIsisNotif OriginatingBuffSize$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsis NotifSystemLevel$*, 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 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

Property name	Value
	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.

30.25 tmnxIsisOwnLSPPurge

Table 664: 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
Source stream	main
Message format string	Own LSP Purge - interface: *$vRtrIfIndex$*, on level: *$tmnxIsisNotifSystemLevel$*, 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.

30.26 tmnxIsisPfxLimitOverloadWarning

Table 665: 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
Source stream	main
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 might go into overload. When the tmnx IsisPrefixLimit is reached and the object tmnxIsisPrefixLimitLogOnly is false, IS-IS will be into overload. There is no direct effect when the object tmnxIsisPrefixLimitLogOnly is true.
Recovery	Increase the IS-IS prefix limit.

30.27 tmnxIsisProtoSuppMismatch

Table 666: 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
Source stream	main

Property name	Value
Message format string	Supported protocol mismatch - supported protocol: *$tmnxIsisNotifProtocolsSupported$*, on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, LSP-id: *$vRtrIsisTrapLSPIDString$*
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.

30.28 tmnxIsisRejectedAdjacency

Table 667: 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
Source stream	main
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.

30.29 tmnxIsisRejectedAdjacencySet

Table 668: tmnxIsisRejectedAdjacencySet properties

Property name	Value
Application name	ISIS
Event ID	2065
Event name	tmnxIsisRejectedAdjacencySet
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.37
Default severity	warning
Source stream	main
Message format string	Failed adj-set on interface: *$tmnxIsisNotifyIfIndex$*, for level:*$tmnxIsisNotifSystemLevel$*, description: *$tmnxIsisNotifyDescription$*
Cause	The tmnxIsisRejectedAdjacencySet notification is sent when an adjacency can not be assigned to an adjacency-set because it does not terminate on the same neighbor node as the other adjacencies. This notification each time the adjacency-set is programmed.
Effect	Adjacency-set nhops will not include this adjacency.
Recovery	Remove the interface from the adjacency-set or change the adjacency-set type to non parallel.

30.30 tmnxIsisRejectedAdjacencySid

Table 669: 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

Property name	Value
Source stream	main
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 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 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.

30.31 tmnxIsisRejectedEndXSid

Table 670: tmnxIsisRejectedEndXSid properties

Property name	Value
Application name	ISIS
Event ID	2069
Event name	tmnxIsisRejectedEndXSid
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.41
Default severity	warning
Source stream	main
Message format string	Failed end-x SID on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, description: *$tmnxIsisNotifyDescription$*
Cause	The tmnxIsisRejectedEndXSid notification is sent when we do not establish a SRv6 End-X SID due to a lack of resources. This should be an edge-triggered notification. We should not send a second notification about end-x SID allocation failure for the same adjacency.
Effect	No effect.

Property name	Value
Recovery	Whenever an end-x SID is released, the released end-x SID can be reused by any other adjacency which is waiting to receive an end-x SID.

30.32 tmnxIsisRejectedPgId

Table 671: tmnxIsisRejectedPgId properties

Property name	Value
Application name	ISIS
Event ID	2070
Event name	tmnxIsisRejectedPgId
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.42
Default severity	warning
Source stream	main
Message format string	Failed PGID on interface: *$vRtrIfIndex$*, for level: *$tmnxIsisNotifSystemLevel$*, description: *$tmnxIsisNotifyDescription$*
Cause	The tmnxIsisRejectedPgId notification is sent when we do not establish a SRv6 adjacency PGID due to a lack of resources. This should be an edge-triggered notification. We should not send a second notification about adjacency PGID allocation failure for the same adjacency.
Effect	No effect.
Recovery	Whenever a PGID is released, the released PGID can be reused by any other adjacency which is waiting to receive a PGID.

30.33 tmnxIsisRoutesExpLmtDropped

Table 672: tmnxIsisRoutesExpLmtDropped properties

Property name	Value
Application name	ISIS

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

30.34 tmnxIsisSequenceNumberSkip

Table 673: 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
Source stream	main
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 without 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.

Property name	Value
Effect	No effect.
Recovery	No recovery is necessary.

30.35 tmnxIsisSidError

Table 674: tmnxIsisSidError properties

Property name	Value
Application name	ISIS
Event ID	2057
Event name	tmnxIsisSidError
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.29
Default severity	minor
Source stream	main
Message format string	*$tmnxIsisNotifyDescription$* SID:*$tmnxIsisPrefixSidValue$*, level: *$tmnxIsisPrefixSidLevel$*, mtid:*$tmnxIsisRouteMtId$*, type:*$tmnxIsis PrefixSidType$*, flags:*$tmnxIsisPrefixSidFlags$*, algo: *$tmnxIsisPrefix SidAlgorithm$*
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

30.36 tmnxIsisSidNotInLabelRange

Table 675: 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
Source stream	main
Message format string	SID not in range of router:*$tmnxIsisNotifPfxSidSysIDString$*, SID: *$tmnxIsisPrefixSidValue$*, startLabel:*$tmnxIsisNotifPfxSidRangeStartLbl$*, maxIdx:*$tmnxIsisNotifPfxSidRangeMaxIdx$* level: *$tmnxIsisPrefixSidLevel$*, mtid:*$tmnxIsisRouteMtId$*, type:*$tmnxIsisPrefixSidType$*, flags:*$tmnxIsisPrefixSidFlags$*, algo: *$tmnxIsisPrefixSidAlgorithm$*
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.
Recovery	Increase the label range or change the SID index to be within the current label range.

30.37 tmnxIsisSidStatsIndexAlloc

Table 676: tmnxIsisSidStatsIndexAlloc properties

Property name	Value
Application name	ISIS
Event ID	2067
Event name	tmnxIsisSidStatsIndexAlloc
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.39
Default severity	warning
Source stream	main

Property name	Value
Message format string	Possible messages: • Statistics Index Allocation status changed to *$tmnxIsisNotifStatsIndexStatus$* for adjacency-set *$tmnxIsisSidStatsAdjSet$* • Statistics Index Allocation status changed to *$tmnxIsisNotifStatsIndexStatus$* for adjacency interface *$tmnxIsisSidStatsIfIndex$* • Statistics Index Allocation status changed to *$tmnxIsisNotifStatsIndexStatus$* for node *$tmnxIsisSidStatsPrefix$*/*$tmnxIsisSidStatsPrefixLength$*
Cause	The tmnxIsisSidStatsIndexAlloc notification is sent when the system is not able to allocate a statistic index to at least one SID. This indication is sent once, i.e. if the system retries to allocate a stat index but fails no new notification is sent. Conversely, in case the system resolves the situation and allocates stat indices to all needed SIDs a notification is sent to indicate that stat allocation is in nominal state.
Effect	No effect.
Recovery	No recovery is necessary.

30.38 tmnxIsisSrgbBadLabelRange

Table 677: 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
Source stream	main
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).

Property name	Value
Effect	The configured Segment Routing tunnels will be wrong.
Recovery	Change the label range to recover.

30.39 tmnxIsisSrv6LocError

Table 678: tmnxIsisSrv6LocError properties

Property name	Value
Application name	ISIS
Event ID	2071
Event name	tmnxIsisSrv6LocError
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.43
Default severity	warning
Source stream	main
Message format string	*$tmnxIsisNotifyDescription$*, level:*$tmnxIsisNotifSystemLevel$*, mtid: *$tmnxIsisRouteMtId$*, algo:*$tmnxIsisSrv6SidAlgorithm$*
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 SRv6 locator.
Effect	The Segment Routing tunnel corresponding to this locator 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 SRv6 tunnels which previously failed the programming operation

30.40 tmnxIsisSrv6StaticSidIfTypeError

Table 679: tmnxIsisSrv6StaticSidIfTypeError properties

Property name	Value
Application name	ISIS
Event ID	2072
Event name	tmnxIsisSrv6StaticSidIfTypeError
SNMP notification prefix and OID	TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.44
Default severity	warning
Source stream	main
Message format string	Possible messages: • Unable to install static SID *$tmnxIsisSrv6SidValue$* with behavior *$tmnxIsisSrv6SidEndpointBehavior$* on interface *$vRtrIfIndex$* of type *$tmnxIsisIfOperType$*, description: *$tmnxIsisNotifyDescription$* • Unable to install static USID *$tmnxIsisSrv6USidValue$* with behavior *$tmnxIsisSrv6USidEndpointBehavior$* on interface *$vRtr IfIndex$* of type *$tmnxIsisIfOperType$*, description: *$tmnxIsisNotify Description$*
Cause	This notification is generated when ISIS receives an end.x/uA-sid from the locator module for an existing interface which is up and type bcast; or when a new ISIS bcast interface is enabled for which an end.x/uA-sid exists in the locator module.
Effect	The static SID will not be programmed in the RTM.
Recovery	No recovery is necessary.

30.41 tmnxIsisVersionSkew

Table 680: 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

Property name	Value
Default severity	warning
Source stream	main
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 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.

30.42 vRtrIsisSpbNbrMultAdjExists

Table 681: 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
Source stream	main
Message format string	SPB multiple adjacency exists for neighbor *$vRtrIsisNbrSysIdString$* on interface *$vRtrIfIndex$* 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 adjacency on another interface.

Property name	Value
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.

30.43 vRtrIsisSpbNbrMultAdjExistsClear

Table 682: vRtrIsisSpbNbrMultAdjExistsClear properties

Property name	Value
Application name	ISIS
Event ID	2026
Event name	vRtrIsisSpbNbrMultAdjExistsClear
SNMP notification prefix and OID	TIMETRA-ISIS-MIB.vRtrIsisNotifications.26
Default severity	warning
Source stream	main
Message format string	SPB multiple adjacency cleared for neighbor *$vRtrIsisNbrSysIdString$* on interface *$vRtrIfIndex$* 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 path computations will be correct.
Recovery	None required.

30.44 vRtrSpbEctFidCfgChg

Table 683: vRtrSpbEctFidCfgChg properties

Property name	Value
Application name	ISIS

Property name	Value
Event ID	2027
Event name	vRtrSpbEctFidCfgChg
SNMP notification prefix and OID	TIMETRA-ISIS-MIB.vRtrIsisNotifications.27
Default severity	warning
Source stream	main
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.

31 L2TP

31.1 tmnxL2tpApFailure

Table 684: 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
Source stream	main
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

31.2 tmnxL2tpIsaMdaVRtrStateChange

Table 685: tmnxL2tpIsaMdaVRtrStateChange properties

Property name	Value
Application name	L2TP
Event ID	2002
Event name	tmnxL2tpIsaMdaVRtrStateChange

Property name	Value
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.2
Default severity	minor
Source stream	main
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

31.3 tmnxL2tpLnsPppNcpFailure

Table 686: 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
Source stream	main
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

31.4 tmnxL2tpLnsSePppSessionFailure

Table 687: tmnxL2tpLnsSePppSessionFailure properties

Property name	Value
Application name	L2TP
Event ID	2003
Event name	tmnxL2tpLnsSePppSessionFailure
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.3
Default severity	warning
Source stream	main
Message format string	Possible messages: • L2TP session *$vRtrID$*: *$tmnxL2tpSeStatusId$*, user *$tmnxL2tpLnsSePppPppUserName$* - *$tmnxL2tpNotifyDescription$* • L2TP session *$vRtrID$*:*$tmnxL2tpSeStatusId$*, user *$tmnxL2tpLnsSePppPppUserName$* (interface *$tmnxL2tpLnsSePppGrpIf$*, 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

31.5 tmnxL2tpPeerUnreachable

Table 688: tmnxL2tpPeerUnreachable properties

Property name	Value
Application name	L2TP
Event ID	2001
Event name	tmnxL2tpPeerUnreachable
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.1

Property name	Value
Default severity	warning
Source stream	main
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

31.6 tmnxL2tpTunnelBlacklisted

Table 689: 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
Source stream	main
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

31.7 tmnxL2tpTunnelSelBlacklistFull

Table 690: 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
Source stream	main
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 configured in tmnxL2tpXtTuSelBlacklistLength, or when the limit is no longer reached.
Effect	N/A
Recovery	N/A

31.8 tmnxL2tpVappVRtrStateChange

Table 691: tmnxL2tpVappVRtrStateChange properties

Property name	Value
Application name	L2TP
Event ID	2004
Event name	tmnxL2tpVappVRtrStateChange
SNMP notification prefix and OID	TIMETRA-L2TP-MIB.tmnxL2tpNotifications.4

Property name	Value
Default severity	minor
Source stream	main
Message format string	The operational state changed to *$tmnxL2tpVappVRtrOperState$*. *$tmnxL2tpNotifyDescription$*.
Cause	The tmnxL2tpVappVRtrStateChange notification is sent when the operational state of a L2TP Virtual Machine within an Extended Service Appliance with respect to a Virtual Router changes.
Effect	N/A
Recovery	N/A

32 LAG

32.1 DynamicCostOff

Table 692: 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
Source stream	main
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.

32.2 DynamicCostOn

Table 693: DynamicCostOn properties

Property name	Value
Application name	LAG
Event ID	2001
Event name	DynamicCostOn

Property name	Value
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.1
Default severity	warning
Source stream	main
Message format string	LAG *$tLagIndex$* entered dynamic-cost mode
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.

32.3 LagPortAddFailed

Table 694: 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
Source stream	main
Message format string	Could not add port *$tmnxPortPortID$* to LAG *$tLagIndex$* because *$tLagNotifyPortAddFailReason$*
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.

32.4 LagPortAddFailureCleared

Table 695: LagPortAddFailureCleared properties

Property name	Value
Application name	LAG
Event ID	2005
Event name	LagPortAddFailureCleared
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.5
Default severity	warning
Source stream	main
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

32.5 LagStateEvent

Table 696: 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
Source stream	main
Message format string	LAG *$tLagIndex$* : *$tLagNotifyAdditionalInfo$*

Property name	Value
Cause	The cause described in this event may influence the LAG state.
Effect	The state of the LAG may change.
Recovery	No action needed.

32.6 LagSubGroupSelected

Table 697: LagSubGroupSelected properties

Property name	Value
Application name	LAG
Event ID	2004
Event name	LagSubGroupSelected
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.4
Default severity	warning
Source stream	main
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.

32.7 tLagAdaptiveLoadbalancingChanged

Table 698: tLagAdaptiveLoadbalancingChanged properties

Property name	Value
Application name	LAG
Event ID	2009

Property name	Value
Event name	tLagAdaptiveLoadbalancingChanged
SNMP notification prefix and OID	TIMETRA-LAG-MIB.tLagNotifications.9
Default severity	warning
Source stream	main
Message format string	LAG *$tLagIndex$* adaptive load balancing changed - *$tLagNotify AdditionalInfo$*
Cause	The tLagAdaptiveLoadbalancingChanged is sent when the re-balancing algorithm modifies the LAG hash bucket allocation.
Effect	A better loadbalancing of the egress traffic on the active lag members.
Recovery	No special recovery action is necessary.

32.8 tLagMemberStateEvent

Table 699: 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
Source stream	main
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.

32.9 tmnxLagBfdMemStateChanged

Table 700: 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
Source stream	main
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.

33 LDAP

33.1 tmnxLdapOperStateChange

Table 701: 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
Source stream	security
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

33.2 tmnxLdapServerOperStateChange

Table 702: tmnxLdapServerOperStateChange properties

Property name	Value
Application name	LDAP
Event ID	2002
Event name	tmnxLdapServerOperStateChange
SNMP notification prefix and OID	TIMETRA-LDAP-MIB.tmnxLdapNotifications.2
Default severity	minor
Source stream	security
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

34 LDP

34.1 vRtrLdpGroupIdMismatch

Table 703: 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
Source stream	main
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

34.2 vRtrLdpNgAddrFecCommMismatch

Table 704: vRtrLdpNgAddrFecCommMismatch properties

Property name	Value
Application name	LDP
Event ID	2021
Event name	vRtrLdpNgAddrFecCommMismatch
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.11

Property name	Value
Default severity	minor
Source stream	main
Message format string	Mismatched community - vRtrID: *$vRtrID$* Community vRtrLdpNgAddr FecCommunity
Cause	A vRtrLdpNgAddrFecCommMismatch notification is generated when two or more peer routers advertising labels for the given address FEC have been assigned differing communities, or some have been assigned communities and some have not. It will also be generated if multiple LDP peer routers have been configured to advertise their local LSR-ID as a FEC, and those peer routers have been assigned differing communities. This notification is rate-limited to at most one notification every 60 seconds.
Effect	This condition indicates that the network is mis-configured, and it is likely that the affected address FEC is not being advertised to the routers which the operator intends.
Recovery	Analyze, check and fix the community configuration for all LDP session-parameters and LDP targeted-session peer-templates in the network to find the error. Start with the configuration on the router generating the notification, and if this is correct, look next at the routers advertising the labels to see if their configuration is correct.

34.3 vRtrLdpNgIfStateChange

Table 705: 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
Source stream	main
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.

34.4 vRtrLdpNgInetIfStateChange

Table 706: 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
Source stream	main
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.

34.5 vRtrLdpNgIpv4InstStateChange

Table 707: vRtrLdpNgIpv4InstStateChange properties

Property name	Value
Application name	LDP
Event ID	2011
Event name	vRtrLdpNgIpv4InstStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.1
Default severity	minor
Source stream	main
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.

34.6 vRtrLdpNgIpv6InstStateChange

Table 708: 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
Source stream	main

Property name	Value
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.
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.

34.7 vRtrLdpNgResourceExhaustion

Table 709: 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
Source stream	main
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.

34.8 vRtrLdpNgSessionStateChange

Table 710: 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
Default severity	minor
Source stream	main
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.

Property name	Value
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 vRtrLdp NgSessOverloadFecType 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 v RtrLdpNgPeerLdpId and vRtrLdpNgSessOverloadState has the value of 'false' for given fec and sub type fec.

34.9 vRtrLdpNgSessMaxFecLimitReached

Table 711: 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
Source stream	main
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

Property name	Value
	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.

34.10 vRtrLdpNgSessMaxFecThresChanged

Table 712: 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
Source stream	main
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

Property name	Value
	configured maximum (vRtrLdpNgSessParamMaxFec) resulting in the generation of vRtrLdpNgSessMaxFecLimitReached notification.
Recovery	Appropriate Configuration changes in local or peer LSR will be required.

34.11 vRtrLdpNgTargPeerStateChange

Table 713: vRtrLdpNgTargPeerStateChange properties

Property name	Value
Application name	LDP
Event ID	2015
Event name	vRtrLdpNgTargPeerStateChange
SNMP notification prefix and OID	TIMETRA-LDP-NG-MIB.tmnxLdpNgNotifications.5
Default severity	minor
Source stream	main
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.

34.12 vRtrLdpStateChange

Table 714: 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
Source stream	main
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

35 LI

35.1 cli_config_io

Table 715: 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
Source stream	li
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.

35.2 cli_unauth_config_io

Table 716: 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

Property name	Value
Default severity	minor
Source stream	li
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	User has entered configuration command for which he is not authorized.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

35.3 cli_unauth_user_io

Table 717: 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
Source stream	li
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.

35.4 cli_user_io

Table 718: 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
Source stream	li
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	A CLI command was entered.
Effect	A CLI command was processed.
Recovery	No recovery is required.

35.5 cli_user_login

Table 719: 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
Source stream	li
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.

35.6 cli_user_login_failed

Table 720: 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
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* failed authentication
Cause	The 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.

35.7 cli_user_login_max_attempts

Table 721: 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
Source stream	li

Property name	Value
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 session 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.

35.8 cli_user_logout

Table 722: 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
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	A user access session was stopped.

Property name	Value
Recovery	No recovery is required.

35.9 destinationDisabled

Table 723: 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
Source stream	li
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.

35.10 destinationEnabled

Table 724: destinationEnabled properties

Property name	Value
Application name	LI
Event ID	2013
Event name	destinationEnabled

Property name	Value
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.3
Default severity	minor
Source stream	li
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.

35.11 ftp_user_login

Table 725: 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
Source stream	li
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

35.12 ftp_user_login_failed

Table 726: 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
Source stream	li
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.

35.13 ftp_user_login_max_attempts

Table 727: 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
Source stream	li
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

Property name	Value
	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 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.

35.14 ftp_user_logout

Table 728: 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
Source stream	li
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

35.15 grpc_auth

Table 729: grpc_auth properties

Property name	Value
Application name	LI
Event ID	2403
Event name	grpc_auth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC authorized
Cause	The user called a RPC in gRPC interface.
Effect	The RPC was processed.
Recovery	No recovery is required.

35.16 grpc_unauth

Table 730: grpc_unauth properties

Property name	Value
Application name	LI
Event ID	2404
Event name	grpc_unauth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC unauthorized

Property name	Value
Cause	The user called a RPC in gRPC interface for which they are not authorized.
Effect	The RPC was not processed.
Recovery	No recovery is required.

35.17 grpc_user_login

Table 731: grpc_user_login properties

Property name	Value
Application name	LI
Event ID	2118
Event name	grpc_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
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

35.18 grpc_user_login_failed

Table 732: grpc_user_login_failed properties

Property name	Value
Application name	LI
Event ID	2120

Property name	Value
Event name	grpc_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
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.

35.19 grpc_user_login_max_attempts

Table 733: grpc_user_login_max_attempts properties

Property name	Value
Application name	LI
Event ID	2121
Event name	grpc_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$tmnxSecNotifyUserName$* from *$tmnxSecNotifyAddr$* attempted more than *$tmnxPasswordAttemptsCount$* times to log in, user locked out for *$tmnxPasswordAttemptsLockoutPeriod$* min
Cause	A Lawful Interception user attempting to connect via gRPC 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 gRPC. The

Property name	Value
	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 gRPC.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. An gRPC session is terminated.
Recovery	No recovery action is required.

35.20 grpc_user_logout

Table 734: grpc_user_logout properties

Property name	Value
Application name	LI
Event ID	2119
Event name	grpc_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
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

35.21 host_snmp_attempts

Table 735: 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
Source stream	li
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) exceeded 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

35.22 md_cli_io

Table 736: md_cli_io properties

Property name	Value
Application name	LI
Event ID	2223
Event name	md_cli_io
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* [session ID *$sessionId$*]: *$prompt$ $command$*
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.

35.23 md_cli_unauth_io

Table 737: md_cli_unauth_io properties

Property name	Value
Application name	LI
Event ID	2224
Event name	md_cli_unauth_io
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* [session ID *$sessionId$*]. Command not allowed for this user: *$prompt$ $command$*
Cause	The user entered a command in MD-CLI for which they are not authorized.
Effect	The MD-CLI command was not processed.
Recovery	No recovery is required.

35.24 mdCommitSucceeded

Table 738: mdCommitSucceeded properties

Property name	Value
Application name	LI
Event ID	2131
Event name	mdCommitSucceeded
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	li
Message format string	Commit by *$userName$* (*$interface$*) from *$srcAddr$* succeeded.

Property name	Value
Cause	The mdCommitSucceeded event is generated when a commit succeeded.
Effect	The commit succeeded.
Recovery	No recovery is necessary.

35.25 mdLiConfigChange

Table 739: mdLiConfigChange properties

Property name	Value
Application name	LI
Event ID	2210
Event name	mdLiConfigChange
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	target='target' operation='operation' value='value'
Cause	A configuration change was applied to the running datastore.
Effect	The configuration changed.
Recovery	No recovery is required.

35.26 mdSaveCommitHistoryFailed

Table 740: mdSaveCommitHistoryFailed properties

Property name	Value
Application name	LI
Event ID	2129

Property name	Value
Event name	mdSaveCommitHistoryFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.91
Default severity	major
Source stream	li
Message format string	Lawful Intercept commit history file write failed: *$fileName$*
Cause	Saving the commit history file failed because of an error.
Effect	The commit history file was not saved.
Recovery	Identify the cause of the failure and save the configuration to save the commit history.

35.27 netconf_auth

Table 741: netconf_auth properties

Property name	Value
Application name	LI
Event ID	2401
Event name	netconf_auth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC authorized
Cause	The user called a RPC in NETCONF interface.
Effect	The RPC was processed.
Recovery	No recovery is required.

35.28 netconf_unauth

Table 742: netconf_unauth properties

Property name	Value
Application name	LI
Event ID	2402
Event name	netconf_unauth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC unauthorized
Cause	The user called a RPC in NETCONF interface for which they are not authorized.
Effect	The RPC was not processed.
Recovery	No recovery is required.

35.29 netconf_user_login

Table 743: netconf_user_login properties

Property name	Value
Application name	LI
Event ID	2125
Event name	netconf_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* logged in

Property name	Value
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required

35.30 netconf_user_login_failed

Table 744: netconf_user_login_failed properties

Property name	Value
Application name	LI
Event ID	2127
Event name	netconf_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
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

35.31 netconf_user_login_max_attempts

Table 745: netconf_user_login_max_attempts properties

Property name	Value
Application name	LI
Event ID	2128

Property name	Value
Event name	netconf_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
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.

35.32 netconf_user_logout

Table 746: netconf_user_logout properties

Property name	Value
Application name	LI
Event ID	2126
Event name	netconf_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Source stream	li
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

35.33 radiusFailed

Table 747: radiusFailed properties

Property name	Value
Application name	LI
Event ID	2124
Event name	radiusFailed
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.28
Default severity	minor
Source stream	li
Message format string	LI for host failed: *$tMirrorNotifyLiDescription$*
Cause	The system sends a radiusFailed notification when it fails to invoke a mirror destination service requested by a Radius server. More details about the failure are indicated in the tMirrorNotifyLiDescription object.
Effect	The mirror destination service could not be created.
Recovery	Recovery, if required, depends on the alarm cause.

35.34 sbiBootLiConfig

Table 748: 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
Source stream	li
Message format string	Lawful Intercept (LI) bootup configuration status: *$sliConfigStatus$*. LI separate: *$sbiLiSeparate$*. LI local save: *$sbiLiLocalSave$*. System last booted time: *$sysUpTime$*.
Cause	The Lawful Intercept (LI) configuration phase following a system reboot is complete. This notification is generated periodically, about once an hour, and provides the status of the LI configuration processing at bootup time as well as the setting of the li-separate and li-local-save BOF flags.
Effect	LI configuration will be missing or incomplete if the LI configuration phase was not completed successfully.
Recovery	If the LI configuration phase was not completed successfully, then restore the LI configuration manually or reboot the router.

35.35 sbiBootMdReadCommitHistoryFailed

Table 749: sbiBootMdReadCommitHistoryFailed properties

Property name	Value
Application name	LI
Event ID	2130
Event name	sbiBootMdReadCommitHistoryFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.92
Default severity	major
Source stream	li

Property name	Value
Message format string	Lawful Intercept commit history file read failed: *$fileName$*
Cause	Reading the Lawful Intercept commit history file failed because of an error.
Effect	The LI commit history file was not read.
Recovery	Identify the cause of the failure and reboot the system.

35.36 snmp_user_set

Table 750: 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
Source stream	li
Message format string	SNMP user from *$srcAddr$> $vbList$*
Cause	A valid SNMP SET request was received.
Effect	The configuration was changed by an SNMP SET operation.
Recovery	No recovery is required.

35.37 sourceDisabled

Table 751: sourceDisabled properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2012
Event name	sourceDisabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.2
Default severity	minor
Source stream	li
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.

35.38 sourceEnabled

Table 752: 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
Source stream	li
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.

35.39 sourceSapChange

Table 753: 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
Source stream	li
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.

35.40 sourceSubscriberChange

Table 754: sourceSubscriberChange properties

Property name	Value
Application name	LI
Event ID	2019

Property name	Value
Event name	sourceSubscriberChange
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.9
Default severity	minor
Source stream	li
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.

35.41 ssh_user_login

Table 755: 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
Source stream	li
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

35.42 ssh_user_login_failed

Table 756: ssh_user_login_failed properties

Property name	Value
Application name	LI
Event ID	2111
Event name	ssh_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	li
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.

35.43 ssh_user_login_max_attempts

Table 757: 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
Source stream	li

Property name	Value
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.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockout Period minutes. An SSH session is terminated.
Recovery	No recovery action is required.

35.44 ssh_user_logout

Table 758: 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
Source stream	li
Message format string	User *$userName$* from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ends.

Property name	Value
Recovery	No recovery is required

35.45 ssiSaveConfigFailed

Table 759: 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	major
Source stream	li
Message format string	Lawful Intercept configuration file write failed: *$fileName$ $reason$*
Cause	Saving the LI configuration failed because of an error.
Effect	The LI configuration was not saved.
Recovery	Identify the cause of the failure and save the LI configuration.

35.46 ssiSaveConfigSucceeded

Table 760: 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	warning

Property name	Value
Source stream	li
Message format string	Lawful Intercept Configuration file saved to: *$fileName$*
Cause	Saving the LI configuration succeeded.
Effect	The LI configuration was saved.
Recovery	No recovery is necessary.

35.47 ssiSyncConfigFailed

Table 761: 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
Source stream	li
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.

35.48 ssiSyncConfigOK

Table 762: 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
Source stream	li
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.

35.49 tFltrLiRsvdBlockRangeChangeEvent

Table 763: tFltrLiRsvdBlockRangeChangeEvent properties

Property name	Value
Application name	LI
Event ID	2038
Event name	tFltrLiRsvdBlockRangeChangeEvent
SNMP notification prefix and OID	TIMETRA-FILTER-MIB.tFilterNotifications.17
Default severity	minor
Source stream	li
Message format string	LI Reserved Block *$tLiReservedBlockName$* range has changed (start-entry *$tLiReservedBlockStart$* size *$tLiReservedBlockSize$*). This change may rearrange filters entries and may temporarily disrupt current interception.

Property name	Value
Cause	This notification was triggered because LI reserved block range has changed.
Effect	LI entries within the LI reserved block may be moved to a new position. Interception of the moved LI filter entries will be temporarily interrupted.
Recovery	No recovery action is required.

35.50 tMirrorDestinationChangeReject

Table 764: tMirrorDestinationChangeReject properties

Property name	Value
Application name	LI
Event ID	2023
Event name	tMirrorDestinationChangeReject
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.14
Default severity	minor
Source stream	li
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.

35.51 tMirrorFilterAssignToItfWarn

Table 765: tMirrorFilterAssignToItfWarn properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2030
Event name	tMirrorFilterAssignToItfWarn
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.19
Default severity	minor
Source stream	li
Message format string	*$tMirrorFilterType$* filter *$tMirrorFilterId$* , which is referred to by Lawful Intercept has been applied on *$tMirrorFilterDirection$* to interface *$tMirrorFilterIfName$* (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.

35.52 tMirrorFilterAssignToSapWarn

Table 766: 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
Source stream	li
Message format string	*$tMirrorFilterType$* filter *$tMirrorFilterId$* , which is referred to by Lawful Intercept has been applied on *$tMirrorFilterDirection$* to SAP *$tMirrorFilterSapEncapValue$* 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.

Property name	Value
Effect	N/A
Recovery	No recovery required.

35.53 tMirrorFilterAssignToSdpWarn

Table 767: 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
Source stream	li
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.
Effect	N/A
Recovery	No recovery required.

35.54 tMirrorLiFltrUnavailSath

Table 768: tMirrorLiFltrUnavailSath properties

Property name	Value
Application name	LI
Event ID	2046

Property name	Value
Event name	tMirrorLiFltrUnavailSath
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.3
Default severity	minor
Source stream	li
Message format string	Lawful Intercept (LI) mirror source *$tMirrorSourceIndex$* SAP matching entry *$tMirrorSourceFilterEntryId$* of filter *$tMirrorSourceFilterId$* has become unavailable to LI mirroring
Cause	This event is raised when Service Activation Testhead (SAT) begins execution on a SAP that matches a filter entry being mirrored, making it unavailable to LI.
Effect	N/A
Recovery	N/A

35.55 tMirrorLiFltrUnavailSathClr

Table 769: tMirrorLiFltrUnavailSathClr properties

Property name	Value
Application name	LI
Event ID	2047
Event name	tMirrorLiFltrUnavailSathClr
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.4
Default severity	minor
Source stream	li
Message format string	Lawful Intercept (LI) mirror source *$tMirrorSourceIndex$* SAP matching entry *$tMirrorSourceFilterEntryId$* of filter *$tMirrorSourceFilterId$* restored to LI mirroring
Cause	This event is raised when Service Activation Testhead (SAT) becomes active on a SAP that matches a filter entry being mirrored, restoring its availability to LI.
Effect	N/A

Property name	Value
Recovery	N/A

35.56 tMirrorLiNat64SubOperStateCh

Table 770: 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
Source stream	li
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.

35.57 tMirrorLiNatL2awSubOperStateCh

Table 771: tMirrorLiNatL2awSubOperStateCh properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2035
Event name	tMirrorLiNatL2awSubOperStateCh
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.25
Default severity	minor
Source stream	li
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.

35.58 tMirrorLiNatLsnSubOperStateCh

Table 772: 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
Source stream	li
Message format string	The state of LI mirror source *$tMirrorSourceIndex$* LSN subscriber (*$vRtrID$*, *$tMirrorLiNatLsnSubAddr$*/*$tMirrorLiNatLsnSubPrefixLength$*) changed to *$tMirrorLiNatLsnSubOperState$*

Property name	Value
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'.
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.

35.59 tMirrorLiPortUnavailSath

Table 773: tMirrorLiPortUnavailSath properties

Property name	Value
Application name	LI
Event ID	2048
Event name	tMirrorLiPortUnavailSath
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.5
Default severity	minor
Source stream	li
Message format string	Lawful Intercept (LI) mirror source *$tMirrorNotifyLiSvcId$* associated port *$tMirrorNotifyLiPortId$* has become unavailable to LI mirroring
Cause	This event is raised when Service Activation Testhead (SAT) begins execution on a port, making it unavailable to LI.
Effect	N/A
Recovery	N/A

35.60 tMirrorLiPortUnavailSathClr

Table 774: tMirrorLiPortUnavailSathClr properties

Property name	Value
Application name	LI
Event ID	2049
Event name	tMirrorLiPortUnavailSathClr
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.6
Default severity	minor
Source stream	li
Message format string	Lawful Intercept (LI) mirror source *$tMirrorNotifyLiSvcId$* associated port *$tMirrorNotifyLiPortId$* restored to LI mirroring
Cause	This event is raised when Service Activation Testhead (SAT) becomes active on a port, restoring its availability to LI.
Effect	N/A
Recovery	N/A

35.61 tMirrorLiSapUnavailSath

Table 775: tMirrorLiSapUnavailSath properties

Property name	Value
Application name	LI
Event ID	2044
Event name	tMirrorLiSapUnavailSath
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.1
Default severity	minor
Source stream	li
Message format string	Lawful Intercept (LI) mirror source *$tMirrorNotifyLiSvcId$* associated SAP *$tMirrorNotifyLiSapEncapValue$* has become unavailable to LI mirroring

Property name	Value
Cause	This event is raised when Service Activation Testhead (SAT) begins execution on a SAP, making it unavailable to LI.
Effect	N/A
Recovery	N/A

35.62 tMirrorLiSapUnavailSathClr

Table 776: tMirrorLiSapUnavailSathClr properties

Property name	Value
Application name	LI
Event ID	2045
Event name	tMirrorLiSapUnavailSathClr
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.2
Default severity	minor
Source stream	li
Message format string	Lawful Intercept (LI) mirror source *$tMirrorNotifyLiSvcId$* associated SAP *$tMirrorNotifyLiSapEncapValue$* restored to LI mirroring
Cause	This event is raised when Service Activation Testhead (SAT) becomes active on a SAP, restoring its availability to LI.
Effect	N/A
Recovery	N/A

35.63 tMirrorLiSrcPortLicInvalid

Table 777: tMirrorLiSrcPortLicInvalid properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2039
Event name	tMirrorLiSrcPortLicInvalid
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.29
Default severity	major
Source stream	li
Message format string	LI Source Port mirroring license is invalid. License failure state is: *$tMirrorSourcePortLicenseState$*
Cause	The system sends a tMirrorLiSrcPortLicExpired notification when the system license no longer supports the use of port mirroring on LI Source elements.
Effect	The LI Source port mirroring capability will be disabled. Existing LI Source configuration including ports will not be deconfigured.
Recovery	An up-to-date SROS license supporting LI Source port mirroring must be applied to restore operation of LI port mirroring.

35.64 tMirrorLiUpIeInvalid

Table 778: tMirrorLiUpIeInvalid properties

Property name	Value
Application name	LI
Event ID	2043
Event name	tMirrorLiUpIeInvalid
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorCupsUpNotifications.3
Default severity	warning
Source stream	li
Message format string	Invalid LI IE received on SCI - *$tMirrorLiNotifyLongDescription$*
Cause	Inconsistent configuration of li-encryption-key on UP and CP system, or insufficient resources for decryption; the details are available in the object tMirrorLiNotifyLongDescription.

Property name	Value
Effect	The creation, deletion or modification of intercept resources for a subscriber failed.
Recovery	Ensure consistent configuration of li-encryption-key on UP and CP.

35.65 tMirrorLiUpSubFailed

Table 779: tMirrorLiUpSubFailed properties

Property name	Value
Application name	LI
Event ID	2041
Event name	tMirrorLiUpSubFailed
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorCupsUpNotifications.1
Default severity	warning
Source stream	li
Message format string	LI set up for UP subscriber *$tMirrorNotifyLiIdentifier$* intercept-id= *$tMirrorNotifyLiInterceptionId$* session-id=*$tMirrorNotifyLiSessionId$* failed - *$tMirrorLiNotifyLongDescription$*
Cause	Detailed information about the exact cause of the notification is available in the object tMirrorLiNotifyLongDescription.
Effect	Any traffic of a CUPS subscriber subject to Lawful Intercept is not intercepted.
Recovery	N/A

35.66 tMirrorLiUpSubSuccess

Table 780: tMirrorLiUpSubSuccess properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2042
Event name	tMirrorLiUpSubSuccess
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorCupsUpNotifications.2
Default severity	warning
Source stream	li
Message format string	LI for UP subscriber *$tMirrorNotifyLiIdentifier$* intercept-id= *$tMirror NotifyLiInterceptionId$* session-id=*$tMirrorNotifyLiSessionId$* is set up
Cause	Not applicable.
Effect	The system is set up to intercept traffic of a CUPS subscriber subject to Lawful Intercept.
Recovery	N/A

35.67 tMirrorLiX2Alarm

Table 781: tMirrorLiX2Alarm properties

Property name	Value
Application name	LI
Event ID	2037
Event name	tMirrorLiX2Alarm
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.27
Default severity	minor
Source stream	li
Message format string	INE *$tMirrorLiNotifyIneIdentifier$* *$tMirrorLiNotifyX2AlarmRank$* X2 alarm *$tMirrorLiNotifyX2AlarmFlag$* at *$tMirrorLiNotifyDateAndTime$*: *$tMirrorLiNotifyLongDescription$*
Cause	The system sends a tMirrorLiX2Alarm notification every time it sends an 'X2Alarm' message on the X2 interface. It signals an event or a condition that affects the operation of the X1, X2 or X3 interface.
Effect	The effect depends on the alarm cause.

Property name	Value
Recovery	Recovery, if required, depends on the alarm cause.

35.68 tMirrorLiXIfLicenseInvalid

Table 782: tMirrorLiXIfLicenseInvalid properties

Property name	Value
Application name	LI
Event ID	2040
Event name	tMirrorLiXIfLicenseInvalid
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.30
Default severity	minor
Source stream	li
Message format string	TCP LI license invalid; please remove x-interface configuration*$tMirrorLiNotifyLongDescription$*
Cause	The system sends a tMirrorLiXIfLicenseInvalid notification when x-interfaces configuration is made while the system license does not support such configuration.
Effect	The values of the objects tMirrorLiX1OperState, tMirrorLiX1OperState and tMirrorLiX1OperState remain 'outOfService'.
Recovery	Remove any X-interfaces configuration.

35.69 tMirrorSourceFilterAssignReject

Table 783: tMirrorSourceFilterAssignReject properties

Property name	Value
Application name	LI
Event ID	2022
Event name	tMirrorSourceFilterAssignReject

Property name	Value
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.13
Default severity	minor
Source stream	li
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.

35.70 tMirrorSourceFilterAssignWarn

Table 784: 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
Source stream	li
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.

Property name	Value
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.

35.71 tMirrorSourceFilterOverruled

Table 785: 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
Source stream	li
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.

35.72 tMirrorSourceIPFltrChangeReject

Table 786: tMirrorSourceIPFltrChangeReject properties

Property name	Value
Application name	LI

Property name	Value
Event ID	2020
Event name	tMirrorSourceIPFltrChangeReject
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.10
Default severity	minor
Source stream	li
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.

35.73 tMirrorSourceIPv6FltrChangeRej

Table 787: 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
Source stream	li
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 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.

35.74 tMirrorSourceLiFilterChanged

Table 788: 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
Source stream	li
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

35.75 tMirrorSourceLiSubProblem

Table 789: 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
Source stream	li
Message format string	Traffic 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.
Recovery	N/A

35.76 tMirrorSourceMacFltrChangeReject

Table 790: 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

Property name	Value
Source stream	li
Message format string	An attempt was blocked to modify filter-entry *$tMirrorSourceFilterEntry Id$* 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.
Effect	The change was blocked.
Recovery	Modifying the filter is only allowed when it is not being referred by any LI action.

35.77 tmnxClear

Table 791: 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
Source stream	li
Message format string	Clear function *$tmnxClearName$* has been run with parameters: *$tmnx ClearParams$*. 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.

35.78 tmnxConfigCreate

Table 792: tmnxConfigCreate properties

Property name	Value
Application name	LI
Event ID	2207
Event name	tmnxConfigCreate
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9
Default severity	warning
Source stream	li
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 an NMS to trigger maintenance polls of the configuration information.Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

35.79 tmnxConfigDelete

Table 793: tmnxConfigDelete properties

Property name	Value
Application name	LI
Event ID	2208
Event name	tmnxConfigDelete
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.10

Property name	Value
Default severity	warning
Source stream	li
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

35.80 tmnxConfigModify

Table 794: tmnxConfigModify properties

Property name	Value
Application name	LI
Event ID	2206
Event name	tmnxConfigModify
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.8
Default severity	warning
Source stream	li
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A

Property name	Value
Recovery	No recovery is necessary.

35.81 tmnxStateChange

Table 795: 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
Source stream	li
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 administrative or operational state of a MIB table entry.
Effect	N/A
Recovery	No recovery is necessary.

36 LLDP

36.1 lldpRemTablesChange

Table 796: lldpRemTablesChange properties

Property name	Value
Application name	LLDP
Event ID	2001
Event name	lldpRemTablesChange
SNMP notification prefix and OID	LLDP-MIB.lldpNotificationPrefix.1
Default severity	minor
Source stream	main
Message format string	LLDP stats remote table has been updated
Cause	N/A
Effect	N/A
Recovery	N/A

36.2 tmnxLldpRemEntryPeerAdded

Table 797: tmnxLldpRemEntryPeerAdded properties

Property name	Value
Application name	LLDP
Event ID	2101
Event name	tmnxLldpRemEntryPeerAdded
SNMP notification prefix and OID	TIMETRA-LLDP-MIB.tmnxLldpNotifs.1

Property name	Value
Default severity	minor
Source stream	main
Message format string	LLDP Remote peer added, local port-id *$ifIndex$*, dest-mac-type *$tmnxLldpRemLocalDestMACAddress$*, remote system name *$tmnxLldpRemSysName$*, remote chassis-id *$tmnxLldpRemChassisId$*, remote port-id *$tmnxLldpRemPortId$*, remote-index *$tmnxLldpRemIndex$*
Cause	The tmnxLldpRemEntryPeerAdded notification is generated when a new remote peer is added to the LLDP.
Effect	N/A
Recovery	N/A

36.3 tmnxLldpRemEntryPeerRemoved

Table 798: tmnxLldpRemEntryPeerRemoved properties

Property name	Value
Application name	LLDP
Event ID	2103
Event name	tmnxLldpRemEntryPeerRemoved
SNMP notification prefix and OID	TIMETRA-LLDP-MIB.tmnxLldpNotifs.3
Default severity	minor
Source stream	main
Message format string	LLDP Remote peer removed, local port-id *$ifIndex$*, dest-mac-type *$tmnxLldpRemLocalDestMACAddress$*, remote system name *$tmnxLldpRemSysName$*, remote chassis-id *$tmnxLldpRemChassisId$*, remote port-id *$tmnxLldpRemPortId$*, remote-index *$tmnxLldpRemIndex$*
Cause	The tmnxLldpRemEntryPeerRemoved notification is generated when a remote peer is deleted from the LLDP.
Effect	N/A
Recovery	N/A

36.4 tmnxLldpRemEntryPeerUpdated

Table 799: tmnxLldpRemEntryPeerUpdated properties

Property name	Value
Application name	LLDP
Event ID	2102
Event name	tmnxLldpRemEntryPeerUpdated
SNMP notification prefix and OID	TIMETRA-LLDP-MIB.tmnxLldpNotifs.2
Default severity	minor
Source stream	main
Message format string	LLDP Remote peer updated, local port-id *$ifIndex$*, dest-mac-type *$tmnxLldpRemLocalDestMACAddress$*, remote system name *$tmnxLldpRemSysName$*, remote chassis-id *$tmnxLldpRemChassisId$*, remote port-id *$tmnxLldpRemPortId$*, remote-index *$tmnxLldpRemIndex$*
Cause	The tmnxLldpRemEntryPeerUpdated notification is generated when a tmnxLldpRemSysName changes for an existing peer
Effect	N/A
Recovery	N/A

36.5 tmnxLldpRemManAddrEntryAdded

Table 800: tmnxLldpRemManAddrEntryAdded properties

Property name	Value
Application name	LLDP
Event ID	2104
Event name	tmnxLldpRemManAddrEntryAdded
SNMP notification prefix and OID	TIMETRA-LLDP-MIB.tmnxLldpNotifs.4
Default severity	minor

Property name	Value
Source stream	main
Message format string	LLDP Remote peer mgmt address added, local-port-id *$ifIndex$*, dest-mac-type *$tmnxLldpRemLocalDestMACAddress$*, remote management address *$tmnxLldpRemManAddr$*, remote-index *$tmnx LldpRemIndex$*
Cause	The tmnxLldpRemManAddrEntryAdded notification is generated when a remote management address is added to the LLDP
Effect	N/A
Recovery	N/A

36.6 tmnxLldpRemManAddrEntryRemoved

Table 801: tmnxLldpRemManAddrEntryRemoved properties

Property name	Value
Application name	LLDP
Event ID	2105
Event name	tmnxLldpRemManAddrEntryRemoved
SNMP notification prefix and OID	TIMETRA-LLDP-MIB.tmnxLldpNotifs.5
Default severity	minor
Source stream	main
Message format string	LLDP Remote peer mgmt address removed, local-port-id *$ifIndex $*, dest-mac-type *$tmnxLldpRemLocalDestMACAddress$*, remote management address *$tmnxLldpRemManAddr$*, remote-index *$tmnx LldpRemIndex$*
Cause	The tmnxLldpRemManAddrEntryRemoved notification is generated when a remote management address is deleted from the LLDP
Effect	N/A
Recovery	N/A

37 LOGGER

37.1 STARTED

Table 802: STARTED properties

Property name	Value
Application name	LOGGER
Event ID	2001
Event name	STARTED
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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 803: tmnxClear properties

Property name	Value
Application name	LOGGER
Event ID	2010
Event name	tmnxClear
SNMP notification prefix and OID	TIMETRA-CLEAR-MIB.tmnxClearNotifications.1

Property name	Value
Default severity	indeterminate
Source stream	main
Message format string	Clear function *$tmnxClearName$* has been run with parameters: *$tmnx ClearParams$*. 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, the managed object was cleared.
Recovery	If failed, check that the managed object exists or that the clear function parameters are correct.

37.3 tmnxCustomEvent1

Table 804: tmnxCustomEvent1 properties

Property name	Value
Application name	LOGGER
Event ID	2020
Event name	tmnxCustomEvent1
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.13
Default severity	critical
Source stream	main
Message format string	*$logCustomEventMessageString$*
Cause	A tmnxCustomEvent1 notification is generated on demand when operator types perform log custom-event from MD interface, or equivalent is received from NETCONF interface, with severity critical.
Effect	tmnxCustomEvent1 notification with all custom set fields is sent to all supported interfaces, Log, NETCONF, SNMP.
Recovery	No action needed.

37.4 tmnxCustomEvent2

Table 805: tmnxCustomEvent2 properties

Property name	Value
Application name	LOGGER
Event ID	2021
Event name	tmnxCustomEvent2
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.14
Default severity	major
Source stream	main
Message format string	*$logCustomEventMessageString$*
Cause	A tmnxCustomEvent2 notification is generated on demand when operator types perform log custom-event from MD interface, or equivalent is received from NETCONF interface, with severity major.
Effect	tmnxCustomEvent2 notification with all custom set fields is sent to all supported interfaces, Log, NETCONF, SNMP.
Recovery	No action needed.

37.5 tmnxCustomEvent3

Table 806: tmnxCustomEvent3 properties

Property name	Value
Application name	LOGGER
Event ID	2022
Event name	tmnxCustomEvent3
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.15
Default severity	minor
Source stream	main

Property name	Value
Message format string	*$logCustomEventMessageString$*
Cause	A tmnxCustomEvent3 notification is generated on demand when operator types perform log custom-event from MD interface, or equivalent is received from NETCONF interface, with severity minor.
Effect	tmnxCustomEvent3 notification with all custom set fields is sent to all supported interfaces, Log, NETCONF, SNMP.
Recovery	No action needed.

37.6 tmnxCustomEvent4

Table 807: tmnxCustomEvent4 properties

Property name	Value
Application name	LOGGER
Event ID	2023
Event name	tmnxCustomEvent4
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.16
Default severity	warning
Source stream	main
Message format string	*$logCustomEventMessageString$*
Cause	A tmnxCustomEvent4 notification is generated on demand when operator types perform log custom-event from MD interface, or equivalent is received from NETCONF interface, with severity warning.
Effect	tmnxCustomEvent4 notification with all custom set fields is sent to all supported interfaces, Log, NETCONF, SNMP.
Recovery	No action needed.

37.7 tmnxCustomEvent5

Table 808: tmnxCustomEvent5 properties

Property name	Value
Application name	LOGGER
Event ID	2024
Event name	tmnxCustomEvent5
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.17
Default severity	cleared
Source stream	main
Message format string	*$logCustomEventMessageString$*
Cause	A tmnxCustomEvent5 notification is generated on demand when operator types perform log custom-event from MD interface, or equivalent is received from NETCONF interface, with severity cleared.
Effect	tmnxCustomEvent5 notification with all custom set fields is sent to all supported interfaces, Log, NETCONF, SNMP.
Recovery	No action needed.

37.8 tmnxCustomEvent6

Table 809: tmnxCustomEvent6 properties

Property name	Value
Application name	LOGGER
Event ID	2025
Event name	tmnxCustomEvent6
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.18
Default severity	indeterminate
Source stream	main
Message format string	*$logCustomEventMessageString$*
Cause	A tmnxCustomEvent6 notification is generated on demand when operator types perform log custom-event from MD interface, or

Property name	Value
	equivalent is received from NETCONF interface, with severity indeterminate.
Effect	tmnxCustomEvent6 notification with all custom set fields is sent to all supported interfaces, Log, NETCONF, SNMP.
Recovery	No action needed.

37.9 tmnxLogAccountingDataLoss

Table 810: 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
Source stream	main
Message format string	Accounting data loss occurred 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

37.10 tmnxLogAdminLocFailed

Table 811: tmnxLogAdminLocFailed properties

Property name	Value
Application name	LOGGER
Event ID	2006
Event name	tmnxLogAdminLocFailed
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.2
Default severity	major
Source stream	main
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

37.11 tmnxLogBackupLocFailed

Table 812: 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
Source stream	main

Property name	Value
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

37.12 tmnxLogEventOverrun

Table 813: 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
Source stream	main
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.

Property name	Value
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

37.13 tmnxLogEventThrottled

Table 814: tmnxLogEventThrottled properties

Property name	Value
Application name	LOGGER
Event ID	2012
Event name	tmnxLogEventThrottled
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.8
Default severity	major
Source stream	main
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

37.14 tmnxLogFileDeleted

Table 815: tmnxLogFileDeleted properties

Property name	Value
Application name	LOGGER
Event ID	2009

Property name	Value
Event name	tmnxLogFileDeleted
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.5
Default severity	minor
Source stream	main
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

37.15 tmnxLogFileRollover

Table 816: 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
Source stream	main
Message format string	Log file *$tmnxLogFileIdPathName$* on compact flash cf*$tmnxLogFileIdOperLocation$* 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 tmnxLogFileIdOperLocation is closed and a new file is created as specified by tmnxLogFileIdAdminLocation and tmnxLogFileIdBackupLoc.
Recovery	No recovery is necessary.

37.16 tmnxLogOnlyEventOverrun

Table 817: tmnxLogOnlyEventOverrun properties

Property name	Value
Application name	LOGGER
Event ID	2018
Event name	tmnxLogOnlyEventOverrun
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	main
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 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

37.17 tmnxLogOnlyEventThrottled

Table 818: tmnxLogOnlyEventThrottled properties

Property name	Value
Application name	LOGGER
Event ID	2016
Event name	tmnxLogOnlyEventThrottled
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	main
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

37.18 tmnxLogSpaceContention

Table 819: 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
Source stream	main
Message format string	Space contention occurred on compact flash cf *$cFlashId$* during I/O for *$subject$*.

Property name	Value
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

37.19 tmnxLogTraceError

Table 820: 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
Source stream	main
Message format string	*$tmnxLogTraceErrorTitle$*: *$tmnxLogTraceErrorMessage$*
Cause	The tmnxLogTraceError notification is generated when a critical level trace error has been detected by the software. There are multiple triggers for such a trace error.
Effect	Effect varies depending on the specific trigger.
Recovery	Contact Nokia Support.

37.20 tmnxStdEventsReplayed

Table 821: 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
Source stream	main
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

37.21 tmnxSysLogTargetProblem

Table 822: tmnxSysLogTargetProblem properties

Property name	Value
Application name	LOGGER
Event ID	2013
Event name	tmnxSysLogTargetProblem
SNMP notification prefix and OID	TIMETRA-LOG-MIB.tmnxLogNotifications.9

Property name	Value
Default severity	major
Source stream	main
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 identified by the tmnxSysLogTargetId.
Recovery	N/A

37.22 tmnxTestEvent

Table 823: 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
Source stream	main
Message format string	Possible messages: • Test event has been generated with system object identifier *$sysObjectID$* System description: *$sysDescr$* • *$tmnxLogEventTestCustomText$*
Cause	The tmnxTestEvent notification is generated when the object tmnxEventTest 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.

Property name	Value
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 MACSEC

38.1 tmnxMacsecCaCreate

Table 824: tmnxMacsecCaCreate properties

Property name	Value
Application name	MACSEC
Event ID	2011
Event name	tmnxMacsecCaCreate
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.11
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* psk-index *$tmnxMacsec PreSharedKeyIndex$* CKN *$tmnxMacsecPreSharedKeyCakName$* created
Cause	A tmnxMacsecCaCreate notification is generated when a connectivity association is created.
Effect	N/A
Recovery	N/A

38.2 tmnxMacsecConfiguredPortCA

Table 825: tmnxMacsecConfiguredPortCA properties

Property name	Value
Application name	MACSEC
Event ID	2001
Event name	tmnxMacsecConfiguredPortCA

Property name	Value
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.1
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* CKN *$tmnxMacsecPreSharedKeyCakName$* configured on port *$tmnxMacsecNotifyPortId$* sub-port *$tmnxMacsecNotifyVlanId$*
Cause	A tmnxMacsecConfiguredPortCA notification is generated when a CA is associated with a port.
Effect	N/A
Recovery	N/A

38.3 tmnxMacsecDisabledPort

Table 826: tmnxMacsecDisabledPort properties

Property name	Value
Application name	MACSEC
Event ID	2004
Event name	tmnxMacsecDisabledPort
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.4
Default severity	minor
Source stream	main
Message format string	MACsec admin disabled on port *$tmnxMacsecPortId$* sub-port *$tmnxMacsecNotifyVlanId$* CA *$tmnxMacsecPortCaName$*
Cause	A tmnxMacsecDisabledPort notification is generated when a port is admin disabled or the associated CA is disabled.
Effect	N/A
Recovery	N/A

38.4 tmnxMacsecDpReplayAttempt

Table 827: tmnxMacsecDpReplayAttempt properties

Property name	Value
Application name	MACSEC
Event ID	2016
Event name	tmnxMacsecDpReplayAttempt
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.16
Default severity	minor
Source stream	main
Message format string	MACsec port *$tmnxMacsecPortId$* sub-port *$tmnxMacsecVlanId$* RxSCI *$tmnxMacsecRxSci$* data packets replay count *$tmnxMacsec RxSCStatsLatePkts$*
Cause	A tmnxMacsecDpReplayAttempt notification is generated every 10 seconds if the counter for detected replay attempts is different from the last time this notification was raised. If the counter has not changed, it will be checked again in 10 seconds.
Effect	N/A
Recovery	N/A

38.5 tmnxMacsecEnabledPort

Table 828: tmnxMacsecEnabledPort properties

Property name	Value
Application name	MACSEC
Event ID	2003
Event name	tmnxMacsecEnabledPort
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.3
Default severity	minor

Property name	Value
Source stream	main
Message format string	MACsec admin enabled on port *$tmnxMacsecPortId$* sub-port *$tmnx MacsecNotifyVlanId$* CA *$tmnxMacsecPortCaName$*
Cause	A tmnxMacsecEnabledPort notification is generated when a port is admin enabled and the associated CA is enabled.
Effect	N/A
Recovery	N/A

38.6 tmnxMacsecMaxPeerLimitCleared

Table 829: tmnxMacsecMaxPeerLimitCleared properties

Property name	Value
Application name	MACSEC
Event ID	2010
Event name	tmnxMacsecMaxPeerLimitCleared
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.10
Default severity	minor
Source stream	main
Message format string	MACsec peer limit cleared on security-zone *$tmnxMacsecNotify SecurityZone$* for peer mi:mac *$tmnxMacsecNotifyPeerMi$*:*$tmnx MacsecMkaPeerListSci$* on port *$tmnxMacsecPortId$* sub-port *$tmnx MacsecVlanId$*
Cause	A tmnxMacsecMaxPeerLimitCleared notification is generated when an MKA session no longer exceeds the maximum number of allowable peers.
Effect	N/A
Recovery	N/A

38.7 tmnxMacsecMaxPeerLimitExceeded

Table 830: tmnxMacsecMaxPeerLimitExceeded properties

Property name	Value
Application name	MACSEC
Event ID	2005
Event name	tmnxMacsecMaxPeerLimitExceeded
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.5
Default severity	minor
Source stream	main
Message format string	MACsec peer limit exceeded on security-zone *$tmnxMacsecNotifySecurityZone$* for peer mi:mac *$tmnxMacsecNotifyPeerMi$*:*$tmnxMacsecMkaPeerListSci$* on port *$tmnxMacsecPortId$* sub-port *$tmnxMacsecVlanId$*
Cause	A tmnxMacsecMaxPeerLimitExceeded notification is generated when an MKA session exceeds the maximum number of allowable peers.
Effect	N/A
Recovery	N/A

38.8 tmnxMacsecMkaReplayAttemptDisc

Table 831: tmnxMacsecMkaReplayAttemptDisc properties

Property name	Value
Application name	MACSEC
Event ID	2015
Event name	tmnxMacsecMkaReplayAttemptDisc
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.15
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecPortCaName$* port *$tmnxMacsecPortId$* sub-port *$tmnxMacsecVlanId$* MACsec MKA packets replay count *$tmnxMacsecMkaStatsPduInvalidNum$*

Property name	Value
Cause	A tmnxMacsecMkaReplayAttemptDisc notification is generated when the replay packet counter increments
Effect	N/A
Recovery	N/A

38.9 tmnxMacsecSakCreate

Table 832: tmnxMacsecSakCreate properties

Property name	Value
Application name	MACSEC
Event ID	2012
Event name	tmnxMacsecSakCreate
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.12
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* CKN *$tmnxMacsec PreSharedKeyCakName$* port *$tmnxMacsecNotifyPortId$* sub-port *$tmnxMacsecNotifyVlanId$* new SAK created as key server AN *$tmnx MacsecNotifyAssociationNum$*
Cause	A tmnxMacsecSakCreate notification is generated when a SAK has been created as a key server.
Effect	N/A
Recovery	N/A

38.10 tmnxMacsecSakDelete

Table 833: tmnxMacsecSakDelete properties

Property name	Value
Application name	MACSEC
Event ID	2017
Event name	tmnxMacsecSakDelete
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.17
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* CKN *$tmnxMacsecPreSharedKeyCakName$* port *$tmnxMacsecNotifyPortId$* sub-port *$tmnxMacsecNotifyVlanId$* SAK deleted AN *$tmnxMacsecNotifyAssociationNum$*
Cause	A tmnxMacsecSakDelete notification is generated when a SAK has been deleted.
Effect	N/A
Recovery	N/A

38.11 tmnxMacsecSakInstalledRx

Table 834: tmnxMacsecSakInstalledRx properties

Property name	Value
Application name	MACSEC
Event ID	2013
Event name	tmnxMacsecSakInstalledRx
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.13
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* CKN *$tmnxMacsecPreSharedKeyCakName$* port *$tmnxMacsecNotifyPortId$* sub-port

Property name	Value
	$tmnxMacsecNotifyVlanId$ new SAK installed AN *$tmnxMacsecNotify AssociationNum$*
Cause	A tmnxMacsecSakInstalledRx notification is generated when a new SAK is installed for receiving
Effect	N/A
Recovery	N/A

38.12 tmnxMacsecSakInstalledTx

Table 835: tmnxMacsecSakInstalledTx properties

Property name	Value
Application name	MACSEC
Event ID	2014
Event name	tmnxMacsecSakInstalledTx
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.14
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* CKN *$tmnxMacsec PreSharedKeyCakName$* port *$tmnxMacsecNotifyPortId$* sub-port *$tmnxMacsecNotifyVlanId$* new SAK activated AN *$tmnxMacsecNotify AssociationNum$*
Cause	A tmnxMacsecSakInstalledTx notification is generated when a new SAK is installed for transmitting
Effect	N/A
Recovery	N/A

38.13 tmnxMacsecUnconfiguredPortCA

Table 836: tmnxMacsecUnconfiguredPortCA properties

Property name	Value
Application name	MACSEC
Event ID	2002
Event name	tmnxMacsecUnconfiguredPortCA
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.2
Default severity	minor
Source stream	main
Message format string	MACsec CA *$tmnxMacsecConnAssocName$* CKN *$tmnxMacsecPreSharedKeyCakName$* unconfigured on port *$tmnxMacsecNotifyPortId$* sub-port *$tmnxMacsecNotifyVlanId$*
Cause	A tmnxMacsecUnconfiguredPortCA notification is generated when a CA is unassociated from a port.
Effect	N/A
Recovery	N/A

38.14 tmnxMkaOperStateChanged

Table 837: tmnxMkaOperStateChanged properties

Property name	Value
Application name	MACSEC
Event ID	2009
Event name	tmnxMkaOperStateChanged
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.9
Default severity	minor
Source stream	main
Message format string	MACsec MKA Operational State changed to: *$tmnxMacsecMkaStatsOperState$* on port *$tmnxMacsecPortId$* sub-port *$tmnxMacsecVlanId$* CA *$tmnxMacsecPortCaName$*

Property name	Value
Cause	A tmnxMkaOperStateChanged notification is generated when an MKA changes operational state.
Effect	N/A
Recovery	N/A

38.15 tmnxMkaPskRollover

Table 838: tmnxMkaPskRollover properties

Property name	Value
Application name	MACSEC
Event ID	2007
Event name	tmnxMkaPskRollover
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.7
Default severity	minor
Source stream	main
Message format string	MACsec port *$tmnxMacsecNotifyPortId$* sub-port *$tmnxMacsecNotifyVlanId$* CA *$tmnxMacsecConnAssocName$* PSK active index *$tmnxMacsecStaticCakActivePsk$*
Cause	A tmnxMkaPskRollover notification is generated when a PSK rollover occurs.
Effect	N/A
Recovery	N/A

38.16 tmnxMkaSessionEnded

Table 839: tmnxMkaSessionEnded properties

Property name	Value
Application name	MACSEC

Property name	Value
Event ID	2008
Event name	tmnxMkaSessionEnded
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.8
Default severity	minor
Source stream	main
Message format string	MACsec MKA session ended with MI:SCI *$tmnxMacsecMkaPeerList Mi$*: *$tmnxMacsecMkaPeerListSci$* on port *$tmnxMacsecPortId$* sub-port *$tmnxMacsecVlanId$* CA *$tmnxMacsecPortCaName$* local MI *$tmnxMacsecMkaStatsMemberId$*
Cause	A tmnxMkaSessionEnded notification is generated when an MKA session is ended.
Effect	N/A
Recovery	N/A

38.17 tmnxMkaSessionEstablished

Table 840: tmnxMkaSessionEstablished properties

Property name	Value
Application name	MACSEC
Event ID	2006
Event name	tmnxMkaSessionEstablished
SNMP notification prefix and OID	TIMETRA-MACSEC-MIB.tmnxMacsecNofitications.6
Default severity	minor
Source stream	main
Message format string	MACsec MKA session established with MI:SCI *$tmnxMacsecMkaPeer ListMi$*: *$tmnxMacsecMkaPeerListSci$* on port *$tmnxMacsecPort Id$* sub-port *$tmnxMacsecVlanId$* CA *$tmnxMacsecPortCaName$* EAPOL-destination *$tmnxMacsecPortEapolDestAddress$* local key-server priority *$tmnxMacsecMkaStatsKeyServerPrio$* peer key-server priority *$tmnxMacsecStaticCakKeyServerPrio$* cipher-suite *$tmnx MacsecConnAssocCipherSuite$* encryption offset *$tmnxMacsecConn AssocEncrptnOffset$* localMI *$tmnxMacsecMkaStatsMemberId$*

Property name	Value
Cause	A tmnxMkaSessionEstablished notification is generated when an MKA session is established.
Effect	N/A
Recovery	N/A

39 MC_REDUNDANCY

39.1 srrpPacketDiscarded

Table 841: 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
Source stream	main
Message format string	Discarded SRRP packet from *$tmnxMcPeerSrcIpAddr$* because *$srrpPacketDiscardReason$*
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

39.2 tMcIPsecDomainActivityStateChg

Table 842: tMcIPsecDomainActivityStateChg properties

Property name	Value
Application name	MC_REDUNDANCY

Property name	Value
Event ID	2046
Event name	tMcIPsecDomainActivityStateChg
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.42
Default severity	warning
Source stream	main
Message format string	Multi-chassis ipsec domain *$tMcIPsecDomainId$* local activity state changed from *$tMcIPsecDomainActyStateOld$* to *$tMcIPsecDomain ActivityState$* because *$tMcIPsecDomainActyStateChR$*, and the active router in the domain is *$tMcIPsecDmCurActiveRouterId$*
Cause	The notification tMcIPsecDomainActivityStateChg is generated whenever activity election state of a domain changes.
Effect	This notification is informational. The effects associated with this notification depend upon the new state of the domain. For example, when a domain becomes active it will begin attracting traffic towards its chassis and will begin to manage IKE sessions for all IPsec tunnels in that domain.
Recovery	No recovery actions are required, although unexpected state transitions often indicate causal fault conditions which may require investigation.

39.3 tMcIpsecDomainProtStatusChg

Table 843: tMcIpsecDomainProtStatusChg properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2047
Event name	tMcIpsecDomainProtStatusChg
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.43
Default severity	warning
Source stream	main

Property name	Value
Message format string	Protection status for the multi-chassis ipsec domain *$tMcIPsecDomainId$* changed to *$tMcIPsecDomainProtectStatus$*
Cause	The notification tMcIpsecDomainProtStatusChg is generated whenever protection status of a ipsec-domain changes.
Effect	This notification is informational. A change in tMcIPsecDomainProtect Status to 'nominal' indicates protection status readiness for switchover.
Recovery	No recovery actions are required.

39.4 tMcPeerIPsecTnlGrpMasterStateChg

Table 844: 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
Default severity	warning
Source stream	main
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.

39.5 tMcPeerIPsecTnlGrpProtStatusChg

Table 845: 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
Source stream	main
Message format string	Protection status for the multi-chassis ipsec peer *$tmnxMcPeerIpAddr $* tunnel-group *$tMcPeerIPsecTnlGrpId$* changed to *$tMcPeerIPsecTnlGrpProtectStatus$*
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.

39.6 tmnxMCEPSessionPsvModeDisabled

Table 846: 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

Property name	Value
Default severity	warning
Source stream	main
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.

39.7 tmnxMCEPSessionPsvModeEnabled

Table 847: 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
Source stream	main
Message format string	Passive-mode for the multi-chassis endpoint peer *$tmnxMcPeerIpAddr $* with source *$tmnxMcPeerSrcIpAddr$* is enabled. Passive-mode with peer has *$tmnxMcPeerEPPsvModeConfigState$*
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

39.8 tmnxMcLagInfoLagChanged

Table 848: 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
Source stream	main
Message format string	tmnxMcLagInfoLagTable: Peer *$tmnxMcPeerIpAddrForNotify$* configuration changed.
Cause	Entries in tmnxMcLagInfoLagTable were changed.
Effect	N/A
Recovery	No recovery is necessary.

39.9 tmnxMcOmcrClientNumEntriesHigh

Table 849: 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
Default severity	minor
Source stream	main

Property name	Value
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 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 tmnxMcPeerWarmStandby 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 tmnxMcsClientNum Entries for the client application specified by tmnxMcsClientApplication. 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 tmnx McPeerIpType and tmnxMcPeerIpAddr indicate the peer that reached the threshold.
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.

39.10 tmnxMcOmcrStatFailedChanged

Table 850: 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
Source stream	main
Message format string	*$tmnxMcOmcrStatClientApplication$* OMCR protection with *$tmnx McOmcrStatAccessProtection$* instance *$tmnxMcOmcrStatIndex$ $tmnxMcOmcrStatFailed$ - $tmnxMcOmcrStatFailure$*
Cause	The notification tmnxMcOmcrStatFailedChanged is generated when the value of the object tmnxMcOmcrStatFailed changes. The most interesting change is from 'notAct' 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	A transition from 'notAct' or 'no' to 'yes' means that the traffic of some or all associated client application entries' is being dropped. For example, all traffic from some or all of the IPOE subscriber hosts protected by a failed SRRP instance is dropped by this system. A transition to 'no' means that the system has successfully allocated resources for the traffic of all associated client application entries. A transition to 'not Act' means that this system is not performing the active role anymore for this access protection instance. For example, the value of the object tmnxSrrpOperState has become different from 'master' for the corresponding instance.
Recovery	There are three recovery actions possible, depending on the reason of the transition of the access protection instance. If it is caused by a problem in the access network, fix that problem, or make additional resources available for this access protection instance. If it is caused by a misconfiguration of this system, correct that, or make additional resources available for this access protection instance.

39.11 tmnxMcPeerEPBfdSessionClose

Table 851: tmnxMcPeerEPBfdSessionClose properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2028
Event name	tmnxMcPeerEPBfdSessionClose

Property name	Value
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.27
Default severity	warning
Source stream	main
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

39.12 tmnxMcPeerEPBfdSessionDown

Table 852: 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
Source stream	main
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

39.13 tmnxMcPeerEPBfdSessionOpen

Table 853: 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
Source stream	main
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 multi-chassis endpoint peer.
Effect	N/A
Recovery	N/A

39.14 tmnxMcPeerEPBfdSessionUp

Table 854: 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

Property name	Value
Source stream	main
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

39.15 tmnxMcPeerEPOperDown

Table 855: 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
Default severity	warning
Source stream	main
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

39.16 tmnxMcPeerEPOperUp

Table 856: 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
Source stream	main
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

39.17 tmnxMcPeerRingsOperStateChanged

Table 857: tmnxMcPeerRingsOperStateChanged properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2022
Event name	tmnxMcPeerRingsOperStateChanged
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.22
Default severity	warning
Source stream	main
Message format string	The MC-Ring operational state of peer *$tmnxMcPeerIpAddr$* changed to *$tmnxMcPeerRingsOperState$*.

Property name	Value
Cause	The notification tmnxMcPeerRingsOperStateChanged is sent when the operational state, with respect to multi-chassis ring operation, of a peer changed. unknown | No rings are configured for this peer. inService | The signaling connection for mc-ring operation | is operational. out OfService | The signaling connection for mc-ring operation | has timed out. transition | Not implemented.
Effect	unknown | None. inService | The signaling 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: unknown | None. inService | None. outOfService | Restore the IP connectivity between the local peer and the remote peer. transition | Not implemented.

39.18 tmnxMcPeerSyncStatusChanged

Table 858: 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
Source stream	main
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.

39.19 tmnxMcRedundancyMismatchDetected

Table 859: 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
Source stream	main
Message format string	*$tmnxMcLagConfigMismatchString$*
Cause	The event is generated when a configuration mismatch is detected.
Effect	N/A
Recovery	No recovery is necessary.

39.20 tmnxMcRedundancyMismatchResolved

Table 860: 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
Default severity	warning
Source stream	main
Message format string	*$tmnxMcLagConfigMismatchString$*
Cause	The event is generated when a configuration mismatch is resolved.

Property name	Value
Effect	N/A
Recovery	No recovery is necessary.

39.21 tmnxMcRedundancyPeerStateChanged

Table 861: 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
Source stream	main
Message format string	The MC-LAG operational status of peer *$tmnxMcPeerIpAddr$* changed to *$tmnxMcLagConfigOperState$*
Cause	The event is generated when the MC lag has changed its operational state.
Effect	N/A
Recovery	No recovery is necessary.

39.22 tmnxMcRingInbCtrlOperStateChgd

Table 862: 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
Source stream	main
Message format string	The MC-Ring operational state of the inband control connection of ring *$tmnxMcPeerIpAddr$*::*$tmnxMcPeerSyncPortSyncTag$* changed to *$tmnxMcRingInfoOperState$*.
Cause	The notification tmnxMcRingInbCtrlOperStateChgd is generated when the operational state of a multi-chassis ring's inband control connection changes. unknown : none 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.

39.23 tmnxMcRingNodeLocOperStateChgd

Table 863: 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
Source stream	main
Message format string	The MC-Ring Node operational state of ring node *$tmnxMcPeer IpAddr$*:: *$tmnxMcPeerSyncPortSyncTag$*::*$tmnxMcRingNodeName $* changed to *$tmnxMcRingNodeInfoLocOperState$* while in-use is *$tmnxMcRingNodeInfoInUse$*.

Property name	Value
Cause	The notification tmnxMcRingNodeLocOperStateChgd is generated upon a change of the operational state of a provisioned ring node as monitored by the local chassis, or when an unprovisioned ring node appears or disappears. unknown : none notProvisioned : the node is configured on the peer but not on this system configErr : the local configuration of the node is incorrect notTested : the ring node connectivity verification is shut down testing : temporary state connected : none disconnected : none
Effect	unknown : none notProvisioned : no effect configErr : no effect not Tested : no effect testing : no effect the effect of the operational state of the ring node depends on the operational state of the ring; 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.

39.24 tmnxMcRingOperStateChanged

Table 864: 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
Source stream	main
Message format string	The MC-Ring operational state of ring *$tmnxMcPeerIpAddr$*:: *$tmnx McPeerSyncPortSyncTag$* changed to *$tmnxMcRingInfoOperState$*.
Cause	The notification tmnxMcRingOperStateChanged is generated when the operational state of a multi-chassis ring changes. unknown : none shutdown : none configErr : none 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

Property name	Value
	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 a conflict between the configuration of this system and its peer or a misconfiguration on one of the ring access node systems testingRing : the inband control connection with the peer is being set up. Waiting for result waitingForPeer : verifying if this ring is configured on the peer
Effect	unknown : none shutdown : the ring brings all SAPs of path-a and path-b operational state 'up' configErr : if there is no peer ring, the ring brings all SAPs on path-a and path-b operational state 'up'; if there is a peer ring, the ring brings all SAPs on path-a and path-b operational state 'down' noPeer : the ring brings all SAPs of path-a and path-b operational state 'up' connected : the ring brings all SAPs of its own path operational state 'up' and all SAPs of the other path operational state 'down' broken : the ring brings all SAPs of path-a and path-b operational state 'up' localBroken : this system brings all SAPs of path-a and path-b operational state 'down' unless they belong to the excluded-path conflict : the ring brings all SAPs of its own path operational state 'up' and all SAPs of the other path 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: unknown : none 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

39.25 tmnxMcSyncClientAlarmCleared

Table 865: tmnxMcSyncClientAlarmCleared properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2006
Event name	tmnxMcSyncClientAlarmCleared

Property name	Value
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.6
Default severity	warning
Source stream	main
Message format string	*$tmnxMcPeerSyncClient$* back in sync with peer *$tmnxMcPeerIpAddrForNotify$*.
Cause	The event is generated when the application has the resources to become in sync again.
Effect	N/A
Recovery	No recovery is necessary.

39.26 tmnxMcSyncClientAlarmRaised

Table 866: 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
Source stream	main
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.

39.27 tmnxMcSyncClockSkewCleared

Table 867: tmnxMcSyncClockSkewCleared properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2020
Event name	tmnxMcSyncClockSkewCleared
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.20
Default severity	warning
Source stream	main
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.

39.28 tmnxMcSyncClockSkewRaised

Table 868: 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

Property name	Value
Source stream	main
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.

39.29 tmnxSrrpBecameBackup

Table 869: tmnxSrrpBecameBackup properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2024
Event name	tmnxSrrpBecameBackup
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.24
Default severity	minor
Source stream	main
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

39.30 tmnxSrrpBfdIntfSessStateChgd

Table 870: 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
Source stream	main
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

39.31 tmnxSrrpDualMaster

Table 871: 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
Source stream	main
Message format string	SRRP ID *$tmnxSrrpOperID$*: Dual Master detected on both peer *$tmnxMcPeerIpAddrForNotify$* / interface *$tmnxMcRemoteGrpIfName ForNotify$* and local *$tmnxMcPeerSrcIpAddr$* / interface *$vRtrIfIndex$*.

Property name	Value
Cause	Both the local and remote SRRP instances are in the master state.
Effect	N/A
Recovery	No recovery is necessary.

39.32 tmnxSrrpDuplicateSubIfAddress

Table 872: 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
Source stream	main
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
Recovery	Resolve IP address conflict.

39.33 tmnxSrrpInstanceIdMismatch

Table 873: tmnxSrrpInstanceIdMismatch properties

Property name	Value
Application name	MC_REDUNDANCY

Property name	Value
Event ID	2009
Event name	tmnxSrrpInstanceIdMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.9
Default severity	warning
Source stream	main
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.

39.34 tmnxSrrpOperDownInvalidMac

Table 874: 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
Source stream	main
Message format string	tmnxSrrpOperDownInvalidMac notification from SRRP id *$tmnxSrrp OperID$* on interface *$vRtrIfIndex$*. SRRP instance is not allowed to be operational.

Property name	Value
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.

39.35 tmnxSrrpOperDownInvalidMacClear

Table 875: 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
Source stream	main
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."

39.36 tmnxSrrpPrivRetailMismatch

Table 876: tmnxSrrpPrivRetailMismatch properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2045
Event name	tmnxSrrpPrivRetailMismatch
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancy Notifications.41
Default severity	warning
Source stream	main
Message format string	SRRP id *$tmnxSrrpOperID$*: mismatch in private retail configuration for service *$tmnxMcNotifyServiceId$ $tmnxMcNotifyTruthValue$* detected/ resolved
Cause	The notification tmnxSrrpPrivRetailMismatch is generated with a value of 'true' for tmnxMcNotifyServiceId when the list of private retail services received through SRRP-MCS synchronization does not match the list that is locally configured on this system, or with a value of 'false' when a matching list of private retail services is received subsequently.
Effect	Downstream traffic received on the standby system for a subscriber associated with a misconfigured retail service can not be forwarded.
Recovery	Restore consistency in the configuration of the private retail services on both systems.

39.37 tmnxSrrpRedIfMismatch

Table 877: 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

Property name	Value
Source stream	main
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.

39.38 tmnxSrrpSapMismatch

Table 878: 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
Source stream	main
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.
Effect	N/A
Recovery	No recovery is necessary.

39.39 tmnxSrrpSapTagMismatch

Table 879: 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
Source stream	main
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.

39.40 tmnxSrrpSubnetMismatch

Table 880: 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
Source stream	main
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 *$vRtrIfIndex$*.

Property name	Value
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.

39.41 tmnxSrrpSubnetMismatchCleared

Table 881: 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
Source stream	main
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.

39.42 tmnxSrrpSystemIpNotSet

Table 882: 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
Source stream	main
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.

39.43 tmnxSrrpTrapNewMaster

Table 883: 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
Source stream	main
Message format string	SRRP instance *$tmnxSrrpOperID$* on interface *$vRtrIfIndex$* (primary address *$tmnxMcPeerIpAddrForNotify$*) changed state to master

Property name	Value
Cause	The sending multi-chassis SRRP instance has transitioned to 'Master' state.
Effect	N/A
Recovery	N/A

40 MCPATH

40.1 tmnxMcPathAvailBwLimitCleared

Table 884: tmnxMcPathAvailBwLimitCleared properties

Property name	Value
Application name	MCPATH
Event ID	2008
Event name	tmnxMcPathAvailBwLimitCleared
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.8
Default severity	minor
Source stream	main
Message format string	The available bandwidth on *$strTmnxMcPathChlPathType$* path on slot/fp *$tmnxMcPathCardSlotNum$*/*$tmnxMcPathFPNum$* is within range limits.
Cause	The available bandwidth limit fell below the maximum limit.
Effect	N/A
Recovery	N/A

40.2 tmnxMcPathAvailBwLimitExceeded

Table 885: tmnxMcPathAvailBwLimitExceeded properties

Property name	Value
Application name	MCPATH
Event ID	2007
Event name	tmnxMcPathAvailBwLimitExceeded

Property name	Value
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.7
Default severity	minor
Source stream	main
Message format string	The available bandwidth on *$strTmnxMcPathChlPathType$* path on slot/fp *$tmnxMcPathCardSlotNum$*/*$tmnxMcPathFPNum$* has reached its maximum limit.
Cause	The available bandwidth limit has been reached.
Effect	N/A
Recovery	N/A

40.3 tmnxMcPathSrcGrpBlackHole

Table 886: tmnxMcPathSrcGrpBlackHole properties

Property name	Value
Application name	MCPATH
Event ID	2005
Event name	tmnxMcPathSrcGrpBlackHole
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.5
Default severity	minor
Source stream	main
Message format string	Channel (*$tmnxMcPathChlSrcAddr$*,*$tmnxMcPathChlGrpAddr$*) for *$tmnxMcPathChlRtrType$* instance *$tmnxMcPathChlRtrInstance$* slot/fp *$tmnxMcPathCardSlotNum$*/ *$tmnxMcPathFPNum$* has been blackholed.
Cause	A source group(S,G) went into a black-hole state."
Effect	N/A
Recovery	N/A

40.4 tmnxMcPathSrcGrpBlackHoleCleared

Table 887: tmnxMcPathSrcGrpBlackHoleCleared properties

Property name	Value
Application name	MCPATH
Event ID	2006
Event name	tmnxMcPathSrcGrpBlackHoleCleared
SNMP notification prefix and OID	TIMETRA-MCAST-PATH-MGMT-MIB.tmnxMcPathNotifications.6
Default severity	minor
Source stream	main
Message format string	Channel (*$tmnxMcPathChlSrcAddr$*,*$tmnxMcPathChlGrpAddr$*) for *$tmnxMcPathChlRtrType$* instance *$tmnxMcPathChlRtrInstance$* slot/fp *$tmnxMcPathCardSlotNum$*/ *$tmnxMcPathFPNum$* is no longer being blackholed.
Cause	A source, group(S,G), went out of the black-hole state.
Effect	N/A
Recovery	N/A

41 MGMT_CORE

41.1 asyncOperationStatusChange

Table 888: asyncOperationStatusChange properties

Property name	Value
Application name	MGMT_CORE
Event ID	2005
Event name	asyncOperationStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	operation-id *$operation-id$* finished with status *$status$*. Presence of messages in the global operations table: error-messages *$error-messages$*, warning-messages *$warning-messages$*, info-messages *$info-messages$*.
Cause	Asynchronous operation finished its execution.
Effect	Full operation results are available.
Recovery	No recovery is required.

41.2 mdAutomaticRollbackFailed

Table 889: mdAutomaticRollbackFailed properties

Property name	Value
Application name	MGMT_CORE
Event ID	2007
Event name	mdAutomaticRollbackFailed

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	critical
Source stream	main
Message format string	Automatic rollback of commit by *$userName$* (*$interface$*) from *$src Addr$* failed.
Cause	The mdAutomaticRollbackFailed event is generated when the automatic rollback after a confirmed commit timeout fails.
Effect	The system does not have the running configuration that was applied before the confirmed commit was executed.
Recovery	Compare the running configuration to the last saved configuration file to determine what configuration has been applied.No recovery is required.

41.3 mdBofConfigChange

Table 890: mdBofConfigChange properties

Property name	Value
Application name	MGMT_CORE
Event ID	2003
Event name	mdBofConfigChange
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	target='target' operation='operation' value='value'
Cause	A configuration change was applied to the BOF running datastore.
Effect	The BOF configuration changed.
Recovery	No recovery is required.

41.4 mdConfigChange

Table 891: mdConfigChange properties

Property name	Value
Application name	MGMT_CORE
Event ID	2001
Event name	mdConfigChange
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	target='target' operation='operation' value='value'
Cause	A configuration change was applied to the running datastore.
Effect	The configuration changed.
Recovery	No recovery is required.

41.5 mdDebugConfigChange

Table 892: mdDebugConfigChange properties

Property name	Value
Application name	MGMT_CORE
Event ID	2004
Event name	mdDebugConfigChange
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	target='target' operation='operation' value='value'
Cause	A configuration change was applied to the debug running datastore.

Property name	Value
Effect	The debug configuration changed.
Recovery	No recovery is required.

41.6 mdOcConfigChange

Table 893: mdOcConfigChange properties

Property name	Value
Application name	MGMT_CORE
Event ID	2002
Event name	mdOcConfigChange
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	target='target' operation='operation' value='value'
Cause	A configuration change was applied to the OpenConfig models in the running datastore.
Effect	The configuration changed.
Recovery	No recovery is required.

41.7 mdRollbackFailed

Table 894: mdRollbackFailed properties

Property name	Value
Application name	MGMT_CORE
Event ID	2008
Event name	mdRollbackFailed

Property name	Value
SNMP notification prefix and OID	N/A
Default severity	critical
Source stream	main
Message format string	rollback of commit by *$userName$* (*$interface$*) from *$srcAddr$* failed.
Cause	The mdRollbackFailed event is generated when the rollback after a confirmed commit cancel fails.
Effect	The system does not have the running configuration that was applied before the confirmed commit was executed.
Recovery	Compare the running configuration to the last saved configuration file to determine what configuration has been applied.No recovery is required.

41.8 syncOperationStatusChange

Table 895: syncOperationStatusChange properties

Property name	Value
Application name	MGMT_CORE
Event ID	2006
Event name	syncOperationStatusChange
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	operation-id *$operation-id$* finished with status *$status$*. Presence of messages in the global operations table: error-messages *$error-messages$*, warning-messages *$warning-messages$*, info-messages *$info-messages$*.
Cause	Synchronous operation finished its execution.
Effect	Operation ID was freed.
Recovery	No recovery is required.

42 MIRROR

42.1 destinationDisabled

Table 896: 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
Source stream	main
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.

42.2 destinationEnabled

Table 897: destinationEnabled properties

Property name	Value
Application name	MIRROR
Event ID	2003
Event name	destinationEnabled

Property name	Value
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.3
Default severity	minor
Source stream	main
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.

42.3 sourceDisabled

Table 898: 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
Source stream	main
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.

42.4 sourceEnabled

Table 899: sourceEnabled properties

Property name	Value
Application name	MIRROR
Event ID	2001
Event name	sourceEnabled
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.1
Default severity	minor
Source stream	main
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.

42.5 sourceIpFilterChange

Table 900: 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
Source stream	main

Property name	Value
Message format string	Mirror source *$tMirrorSourceIndex$* associated IP filter *$tMirrorSource FilterId$* entry *$tMirrorSourceFilterEntryId$* has been *$tMirrorSource ChangeType$*
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.

42.6 sourceMacFilterChange

Table 901: 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
Source stream	main
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.

42.7 sourceSapChange

Table 902: 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
Source stream	main
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.
Recovery	Modify the configuration of the associated SAP to restore the desired mirrored traffic.

42.8 sourceSubscriberChange

Table 903: 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
Source stream	main

Property name	Value
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.

42.9 tMirrorFltrUnavailSath

Table 904: tMirrorFltrUnavailSath properties

Property name	Value
Application name	MIRROR
Event ID	2025
Event name	tMirrorFltrUnavailSath
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.3
Default severity	minor
Source stream	main
Message format string	Mirror source *$tMirrorSourceIndex$* SAP matching entry *$tMirror SourceFilterEntryId$* of filter *$tMirrorSourceFilterId$* has become unavailable to mirroring
Cause	This event is raised when Service Activation Testhead (SAT) begins execution on a SAP that matches a filter entry being mirrored, making it unavailable to mirroring.
Effect	N/A
Recovery	N/A

42.10 tMirrorFltrUnavailSathClr

Table 905: tMirrorFltrUnavailSathClr properties

Property name	Value
Application name	MIRROR
Event ID	2026
Event name	tMirrorFltrUnavailSathClr
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.4
Default severity	minor
Source stream	main
Message format string	Mirror source *$tMirrorSourceIndex$* SAP matching entry *$tMirror SourceFilterEntryId$* of filter *$tMirrorSourceFilterId$* restored to mirroring
Cause	This event is raised when Service Activation Testhead (SAT) becomes active on a SAP that matches a filter entry being mirrored, restoring its availability to mirroring.
Effect	N/A
Recovery	N/A

42.11 tMirrorPortUnavailSath

Table 906: tMirrorPortUnavailSath properties

Property name	Value
Application name	MIRROR
Event ID	2027
Event name	tMirrorPortUnavailSath
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.5
Default severity	minor
Source stream	main
Message format string	Mirror source *$tMirrorSourceIndex$* associated port *$tMirrorSourcePort Index$* has become unavailable to mirroring

Property name	Value
Cause	This event is raised when Service Activation Testhead (SAT) begins execution on a port, making it unavailable to mirroring.
Effect	N/A
Recovery	N/A

42.12 tMirrorPortUnavailSathClr

Table 907: tMirrorPortUnavailSathClr properties

Property name	Value
Application name	MIRROR
Event ID	2028
Event name	tMirrorPortUnavailSathClr
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.6
Default severity	minor
Source stream	main
Message format string	Mirror source *$tMirrorSourceIndex$* associated port *$tMirrorSourcePort Index$* restored to mirroring
Cause	This event is raised when Service Activation Testhead (SAT) becomes active on a port, restoring its availability to mirroring.
Effect	N/A
Recovery	N/A

42.13 tMirrorSapUnavailSath

Table 908: tMirrorSapUnavailSath properties

Property name	Value
Application name	MIRROR

Property name	Value
Event ID	2023
Event name	tMirrorSapUnavailSath
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.1
Default severity	minor
Source stream	main
Message format string	Mirror source *$tMirrorSourceIndex$* associated SAP *$tMirrorSource SapEncapValue$* has become unavailable to mirroring
Cause	This event is raised when Service Activation Testhead (SAT) begins execution on a SAP, making it unavailable to mirroring.
Effect	N/A
Recovery	N/A

42.14 tMirrorSapUnavailSathClr

Table 909: tMirrorSapUnavailSathClr properties

Property name	Value
Application name	MIRROR
Event ID	2024
Event name	tMirrorSapUnavailSathClr
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.2
Default severity	minor
Source stream	main
Message format string	Mirror source *$tMirrorSourceIndex$* associated SAP *$tMirrorSource SapEncapValue$* restored to mirroring
Cause	This event is raised when Service Activation Testhead (SAT) becomes active on a SAP, restoring its availability to mirroring.
Effect	N/A
Recovery	N/A

42.15 tMirrorSourceIpv6FilterChange

Table 910: 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
Source stream	main
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.

43 MLD

43.1 vRtrMldGrpIfSapCModeRxQueryMism

Table 911: 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
Source stream	main
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

43.2 vRtrMldGrpIfSapMaxGrpsLimExceed

Table 912: vRtrMldGrpIfSapMaxGrpsLimExceed properties

Property name	Value
Application name	MLD
Event ID	2012
Event name	vRtrMldGrpIfSapMaxGrpsLimExceed
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.12
Default severity	warning
Source stream	main
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

43.3 vRtrMldGrpIfSapMaxGrpSrcLimExcd

Table 913: 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
Source stream	main
Message format string	Max group sources exceeded *$vRtrMldGrpIfSapMaxGrpSources$* for SAP

Property name	Value
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

43.4 vRtrMldGrpIfSapMaxSrcsLimExceed

Table 914: 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
Source stream	main
Message format string	Max number of sources 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

43.5 vRtrMldGrpIfSapMcacPlcyDropped

Table 915: 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
Source stream	main
Message format string	MLD group *$vRtrMldNotifyGrpAddr$* dropped because applying policy *$vRtrMldNotifyMcacPolicyName$*
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
Recovery	N/A

43.6 vRtrMldGrpIfSapRxQueryVerMism

Table 916: 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
Source stream	main
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.

Property name	Value
	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

43.7 vRtrMldHostCModeRxQueryMismatch

Table 917: 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
Source stream	main
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

43.8 vRtrMldHostInstantiationFail

Table 918: 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
Source stream	main
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

43.9 vRtrMldHostMaxGrpsLimitExceeded

Table 919: 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
Source stream	main
Message format string	*$vRtrMldHostMaxGroups$* exceeded on FwdSvdId *$vRtrMldHostFwd SvcId$*, GrpIfId *$vRtrMldHostGrpIfId$*

Property name	Value
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

43.10 vRtrMldHostMaxGrpSrcsLimitExcd

Table 920: 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
Source stream	main
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 group sources is equal to vRtrMldHostMaxGrpSources, the maximum number of group sources per group supported on the host.
Effect	N/A
Recovery	N/A

43.11 vRtrMldHostMaxSrcsLimitExceeded

Table 921: 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
Source stream	main
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

43.12 vRtrMldHostMcacPlcyDropped

Table 922: vRtrMldHostMcacPlcyDropped properties

Property name	Value
Application name	MLD
Event ID	2007
Event name	vRtrMldHostMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.7
Default severity	warning
Source stream	main
Message format string	MLD group *$vRtrMldNotifyGrpAddr$* dropped on host *$vRtrMldHost SubscriberId$* after applying policy *$vRtrMldNotifyMcacPolicyName$*

Property name	Value
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

43.13 vRtrMldHostQryIntervalConflict

Table 923: 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
Source stream	main
Message format string	MLD-policy query intervals violated for Host on GrpIf
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

43.14 vRtrMldHostRxQueryVerMismatch

Table 924: vRtrMldHostRxQueryVerMismatch properties

Property name	Value
Application name	MLD

Property name	Value
Event ID	2009
Event name	vRtrMldHostRxQueryVerMismatch
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.9
Default severity	warning
Source stream	main
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

43.15 vRtrMldIfCModeRxQueryMismatch

Table 925: 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
Source stream	main
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.

43.16 vRtrMldIfRxQueryVerMismatch

Table 926: 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
Source stream	main
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.

43.17 vRtrMldMaxGrpsLimitExceeded

Table 927: vRtrMldMaxGrpsLimitExceeded properties

Property name	Value
Application name	MLD

Property name	Value
Event ID	2003
Event name	vRtrMldMaxGrpsLimitExceeded
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.3
Default severity	warning
Source stream	main
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

43.18 vRtrMldMaxGrpSrcsLimitExceeded

Table 928: 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
Source stream	main
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

Property name	Value
Recovery	N/A

43.19 vRtrMldMaxSrcsLimitExceeded

Table 929: 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
Source stream	main
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

43.20 vRtrMldMcacPlcyDropped

Table 930: vRtrMldMcacPlcyDropped properties

Property name	Value
Application name	MLD
Event ID	2004
Event name	vRtrMldMcacPlcyDropped

Property name	Value
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.4
Default severity	warning
Source stream	main
Message format string	MLD group *$vRtrMldNotifyGrpAddr$* dropped after applying *$vRtrMld IfMcacPolicyName$*
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
Recovery	N/A

43.21 vRtrMldSlaProfInstMcacPlcyDrop

Table 931: vRtrMldSlaProfInstMcacPlcyDrop properties

Property name	Value
Application name	MLD
Event ID	2021
Event name	vRtrMldSlaProfInstMcacPlcyDrop
SNMP notification prefix and OID	TIMETRA-MLD-MIB.vRtrMldNotifications.21
Default severity	warning
Source stream	main
Message format string	MLD group/source *$vRtrMldNotifyGrpAddr$*/*$vRtrMldNotifySrcAddr$* dropped for SLA profile instance subscriber *$tmnxSubIdent$* SAP *$sap NotifyEncapValue$* SLA profile *$tmnxSubNotifSLAProfName$* group *$tmnxSubNotifSpiGroupId$* due to of MCAC policy *$vRtrMldNotifyMcac PolicyName$* instance *$vRtrID$*, reason *$vRtrMldNotifyDescription$*
Cause	The vRtrMldSlaProfInstMcacPlcyDrop event is generated when an MLD group is dropped on a given SLA profile instance because of applying the multicast CAC policy given by vRtrMldNotifyMcacPolicy Name.
Effect	The SLA profile instance user cannot receive traffic from the MLD group.

Property name	Value
Recovery	Dropping a multicasts group may be an expected effect of access control; if not, the access control configuration must be modified.

44 MLD_SNOOPING

44.1 sapMldSnpgGrpLimitExceeded

Table 932: 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
Source stream	main
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

44.2 sapMldSnpgMcsFailure

Table 933: sapMldSnpgMcsFailure properties

Property name	Value
Application name	MLD_SNOOPING
Event ID	2003
Event name	sapMldSnpgMcsFailure

Property name	Value
SNMP notification prefix and OID	TIMETRA-MLD-SNOOPING-MIB.tmnxMldSnpgSapNotifications.2
Default severity	warning
Source stream	main
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

44.3 sdpBndMldSnpgGrpLimitExceeded

Table 934: 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
Source stream	main
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

45 MPLS

45.1 mplsTunnelDown

Table 935: 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
Source stream	main
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.

45.2 mplsTunnelReoptimized

Table 936: mplsTunnelReoptimized properties

Property name	Value
Application name	MPLS
Event ID	2006
Event name	mplsTunnelReoptimized

Property name	Value
SNMP notification prefix and OID	MPLS-TE-MIB.mplsTeNotifyPrefix.4
Default severity	warning
Source stream	main
Message format string	Tunnel *$mplsTunnelName$* is reoptimized
Cause	A tunnel is reoptimized. If the actual path is used, then this object MAY contain the new path for this tunnel sometime after this trap is issued by the agent.
Effect	Service is affected.
Recovery	No recovery is required.

45.3 mplsTunnelRerouted

Table 937: 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
Source stream	main
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 sometime after this trap is issued by the agent.
Effect	Service is affected.
Recovery	No recovery is required.

45.4 mplsTunnelUp

Table 938: mplsTunnelUp properties

Property name	Value
Application name	MPLS
Event ID	2003
Event name	mplsTunnelUp
SNMP notification prefix and OID	MPLS-TE-MIB.mplsTeNotifyPrefix.1
Default severity	warning
Source stream	main
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.

45.5 mplsXCDown

Table 939: 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
Source stream	main

Property name	Value
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.

45.6 mplsXCUp

Table 940: mplsXCUp properties

Property name	Value
Application name	MPLS
Event ID	2001
Event name	mplsXCUp
SNMP notification prefix and OID	MPLS-LSR-MIB.mplsLsrNotifyPrefix.1
Default severity	warning
Source stream	main
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.

45.7 tmnxMplsResourceExhausted

Table 941: tmnxMplsResourceExhausted properties

Property name	Value
Application name	MPLS
Event ID	2039
Event name	tmnxMplsResourceExhausted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.33
Default severity	critical
Source stream	main
Message format string	Usage of MPLS *$tmnxNotifyMplsResourceType$* resources has reached the maximum limit.
Cause	The tmnxMplsResourceExhausted notification is generated when the usage of the resource specified by tmnxNotifyMplsResourceType has reached the maximum limit.
Effect	The utilization of the specified resource has reached its limit.
Recovery	Intervention may be required to recover resources.

45.8 tmnxMplsResourceHighUsage

Table 942: tmnxMplsResourceHighUsage properties

Property name	Value
Application name	MPLS
Event ID	2038
Event name	tmnxMplsResourceHighUsage
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.32
Default severity	major
Source stream	main
Message format string	Usage of MPLS *$tmnxNotifyMplsResourceType$* resources has reached or exceeded *$tmnxNotifyMplsResourceUsagePct$*% threshold.

Property name	Value
Cause	The tmnxMplsResourceHighUsage notification is generated when the usage of the resource specified by tmnxNotifyMplsResourceType has reached or exceeded the warning threshold specified by tmnxNotify MplsResourceUsagePct.
Effect	The specified resource has reached or exceeded the warning threshold.
Recovery	There is no recovery required for this notification.

45.9 tmnxMplsResourceRecovered

Table 943: tmnxMplsResourceRecovered properties

Property name	Value
Application name	MPLS
Event ID	2040
Event name	tmnxMplsResourceRecovered
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.34
Default severity	minor
Source stream	main
Message format string	Usage of MPLS *$tmnxNotifyMplsResourceType$* resources has dropped below *$tmnxNotifyMplsResourceUsagePct$*% threshold.
Cause	The tmnxMplsResourceRecovered notification is generated when the usage of the resource specified by tmnxNotifyMplsResourceType drops below the warning threshold specified by tmnxNotifyMplsResource UsagePct. This trap is generated only if the tmnxMplsResourceHigh Usage notification or the tmnxMplsResourceExhausted notification had been generated earlier.
Effect	The utilization of the specified resource has dropped below the warning threshold.
Recovery	There is no recovery required for this notification.

45.10 vRtrMplsIfIPv6StateChange

Table 944: vRtrMplsIfIPv6StateChange properties

Property name	Value
Application name	MPLS
Event ID	2032
Event name	vRtrMplsIfIPv6StateChange
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.26
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$* is in administrative state: *$vRtrMplsIfAdmin State$*, IPv6 operational state: *$vRtrMplsIfV6OperState$*
Cause	The vRtrMplsIPv6StateChange notification is generated when MPLS interface changes state.
Effect	The SR-TE LSPs with IPv6 addresses transition state.
Recovery	There is no recovery required for this notification.

45.11 vRtrMplsIfStateChange

Table 945: 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
Source stream	main

Property name	Value
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.

45.12 vRtrMplsIPv6StateChange

Table 946: vRtrMplsIPv6StateChange properties

Property name	Value
Application name	MPLS
Event ID	2031
Event name	vRtrMplsIPv6StateChange
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.25
Default severity	minor
Source stream	main
Message format string	Instance is in administrative state: *$vRtrMplsGeneralAdminState$*, IPv6 operational state: *$vRtrMplsGeneralV6OperState$*
Cause	The vRtrMplsIPv6StateChange notification is generated when MPLS protocol instance changes state.
Effect	The SR-TE LSPs with IPv6 addresses transition state.
Recovery	There is no recovery required for this notification.

45.13 vRtrMplsLspActivePathChanged

Table 947: 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
Source stream	main
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.

45.14 vRtrMplsLspDown

Table 948: vRtrMplsLspDown properties

Property name	Value
Application name	MPLS
Event ID	2010
Event name	vRtrMplsLspDown

Property name	Value
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.4
Default severity	warning
Source stream	main
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.

45.15 vRtrMplsLspManualSwitchFailure

Table 949: vRtrMplsLspManualSwitchFailure properties

Property name	Value
Application name	MPLS
Event ID	2034
Event name	vRtrMplsLspManualSwitchFailure
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.28
Default severity	minor
Source stream	main
Message format string	Manual switch for LSP *$lspName$* failed because *$vRtrMplsLsp ManualSwFailReason$*
Cause	The vRtrMplsLspManualSwitchFailure notification is generated to report an unsuccessful manually triggered active path switch for the LSP. The reason for the failure is specified by vRtrMplsLspManual SwFailReason.
Effect	The manually triggered active path switch failed for the LSP.
Recovery	vRtrMplsLspManualSwFailReason will help the user troubleshoot the failure. The user can attempt to manually switch the LSP again.

45.16 vRtrMplsLspPathDown

Table 950: 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
Source stream	main
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.

45.17 vRtrMplsLspPathLstFillReoptElig

Table 951: vRtrMplsLspPathLstFillReoptElig properties

Property name	Value
Application name	MPLS
Event ID	2022
Event name	vRtrMplsLspPathLstFillReoptElig
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.16
Default severity	warning
Source stream	main
Message format string	Better least-fill metric for path *$lspPathName$* is *$trapStatus$*. *$bandwidthChange$*

Property name	Value
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

45.18 vRtrMplsLspPathManualDegStateChg

Table 952: vRtrMplsLspPathManualDegStateChg properties

Property name	Value
Application name	MPLS
Event ID	2035
Event name	vRtrMplsLspPathManualDegStateChg
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.29
Default severity	minor
Source stream	main
Message format string	Manually degraded state changed to *$vRtrMplsLspPathManDegState$* for LSP path *$lspPathName$*
Cause	The vRtrMplsLspPathManualDegStateChg notification is generated when the manually degraded state of the LSP Path changes to a manually triggered active path switch for the LSP.
Effect	The manually degraded state changed for the LSP path.
Recovery	There is no recovery required for this notification.

45.19 vRtrMplsLspPathMbbStatusEvent

Table 953: 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
Source stream	main
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

45.20 vRtrMplsLspPathRerouted

Table 954: 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
Source stream	main
Message format string	LSP path *$lspPathName$* rerouted
Cause	An LSP Path has been rerouted.
Effect	N/A

Property name	Value
Recovery	N/A

45.21 vRtrMplsLspPathResignaled

Table 955: 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
Source stream	main
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

45.22 vRtrMplsLspPathSoftPreempted

Table 956: vRtrMplsLspPathSoftPreempted properties

Property name	Value
Application name	MPLS
Event ID	2021
Event name	vRtrMplsLspPathSoftPreempted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.15

Property name	Value
Default severity	warning
Source stream	main
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

45.23 vRtrMplsLspPathUp

Table 957: 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
Source stream	main
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.

45.24 vRtrMplsLspResourceExhaustion

Table 958: vRtrMplsLspResourceExhaustion properties

Property name	Value
Application name	MPLS
Event ID	2033
Event name	vRtrMplsLspResourceExhaustion
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.27
Default severity	minor
Source stream	main
Message format string	MPLS received a notification that *$vRtrMplsResourceType$* is exhausted for router: *$vRtrID$*, lsp: *$vRtrMplsLspName$*
Cause	The vRtrMplsLspResourceExhaustion notification is generated when CPM or data path resource specified by vRtrMplsResourceType is exhausted.
Effect	If vRtrMplsResourceType is 'egressStatistics', LSP path egress statistics will not be collected.
Recovery	Appropriate config changes in the system may be required to free up the resources. Once the resources are available and vRtrMpls ResourceType is 'egressStatistics' and vRtrMplsLspType is 'srTe', lsp egress-statistics admin down and up will be needed to bring up lsp path egress-statistics.

45.25 vRtrMplsLspSwitchStbyFailure

Table 959: 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
Source stream	main

Property name	Value
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.

45.26 vRtrMplsLspUp

Table 960: 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
Source stream	main
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.
Recovery	No recovery is required.

45.27 vRtrMplsNodeInIgpOverload

Table 961: 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
Source stream	main
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.

45.28 vRtrMplsNodeInIgpOverloadIpv6

Table 962: vRtrMplsNodeInIgpOverloadIpv6 properties

Property name	Value
Application name	MPLS
Event ID	2037
Event name	vRtrMplsNodeInIgpOverloadIpv6
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.31
Default severity	minor
Source stream	main
Message format string	MPLS received a notification that *$vRtrMplsIgpOverloadIgpType$* is in overload on router *$vRtrMplsIgpOverloadRtrAddr$*.

Property name	Value
Cause	The vRtrMplsNodeInIgpOverloadIpv6 notification is generated when MPLS gets a notification that a node is in IGP overload state.
Effect	The LSPs with IPv6 addresses transiting through nodes that are in IGP overload state are teardown.
Recovery	There is no recovery required for this notification.

45.29 vRtrMplsP2mpInstanceDown

Table 963: 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
Source stream	main
Message format string	P2MP instance *$insName$* LSP *$lspName$* is operationally disabled ('shutdown') because *$vRtrMplsP2mpInstNotifReasonCode$*
Cause	A P2MP instance under LSP transitioned out of 'inService' state to any other state.
Effect	Service is affected.
Recovery	No recovery is required.

45.30 vRtrMplsP2mpInstanceResignaled

Table 964: vRtrMplsP2mpInstanceResignaled properties

Property name	Value
Application name	MPLS

Property name	Value
Event ID	2023
Event name	vRtrMplsP2mpInstanceResignaled
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.17
Default severity	warning
Source stream	main
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.

45.31 vRtrMplsP2mpInstanceUp

Table 965: 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
Source stream	main
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.

45.32 vRtrMplsResignalTimerExpired

Table 966: 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
Source stream	main
Message format string	MPLS resignal timer expired.
Cause	MPLS resignal timer expired
Effect	N/A
Recovery	No recovery is required.

45.33 vRtrMplsS2lSubLspDown

Table 967: vRtrMplsS2lSubLspDown properties

Property name	Value
Application name	MPLS
Event ID	2018
Event name	vRtrMplsS2lSubLspDown
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.12
Default severity	warning
Source stream	main
Message format string	S2L path *$s2lName$* to *$vRtrMplsS2lSubLspNtDstAddr$* for P2MP instance *$insName$* LSP *$lspName$* is operationally disabled ('shutdown') because *$vRtrMplsS2lSubLspFailCode$*

Property name	Value
Cause	A S2L Path transitioned out of 'inService' state to any other state.
Effect	Service is affected.
Recovery	No recovery is required.

45.34 vRtrMplsS2lSubLspPreempted

Table 968: vRtrMplsS2lSubLspPreempted properties

Property name	Value
Application name	MPLS
Event ID	2036
Event name	vRtrMplsS2lSubLspPreempted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.30
Default severity	minor
Source stream	main
Message format string	S2L path *$s2lName$* to *$vRtrMplsS2lSubLspNtDstAddr$* for P2MP instance *$insName$* for LSP *$lspName$* preempted
Cause	The vRtrMplsS2lSubLspPreempted notification is generated when an S2l sub LSP is soft-preempted.
Effect	If applicable, soft-preemption MBB will be started to resignal the S2l sub LSP. If the S2l sub LSP has not been resignaled by the time the preemption timer expires, the S2l will be torn down.
Recovery	There is no recovery required for this notification.

45.35 vRtrMplsS2lSubLspRerouted

Table 969: vRtrMplsS2lSubLspRerouted properties

Property name	Value
Application name	MPLS

Property name	Value
Event ID	2019
Event name	vRtrMplsS2lSubLspRerouted
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.13
Default severity	warning
Source stream	main
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

45.36 vRtrMplsS2lSubLspResignaled

Table 970: vRtrMplsS2lSubLspResignaled properties

Property name	Value
Application name	MPLS
Event ID	2020
Event name	vRtrMplsS2lSubLspResignaled
SNMP notification prefix and OID	TIMETRA-MPLS-MIB.tmnxMplsNotifications.14
Default severity	warning
Source stream	main
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

45.37 vRtrMplsS2lSubLspUp

Table 971: 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
Source stream	main
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.

45.38 vRtrMplsStateChange

Table 972: 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
Source stream	main

Property name	Value
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.

45.39 vRtrMplsXCBundleChange

Table 973: 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
Source stream	main
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.
Effect	RSVP sessions represented by bits in vRtrMplsXCNotifRednIndicesBit Map changed state on this router instance.
Recovery	There is no recovery required for this notification.

46 MPLS_TP

46.1 vRtrMplsTpLspActivePathChange

Table 974: 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
Source stream	main
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 vice 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.

46.2 vRtrMplsTpLspActivePathUp

Table 975: vRtrMplsTpLspActivePathUp properties

Property name	Value
Application name	MPLS_TP
Event ID	2005
Event name	vRtrMplsTpLspActivePathUp

Property name	Value
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.5
Default severity	minor
Source stream	main
Message format string	TP Tunnel *$TpLspName$* active on *$vRtrMplsTpLspPathIndex$* path
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.

46.3 vRtrMplsTpLspPtTypeMismatchAlarm

Table 976: 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
Source stream	main
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

46.4 vRtrMplsTpLspPtTypeMismatchClear

Table 977: vRtrMplsTpLspPtTypeMismatchClear properties

Property name	Value
Application name	MPLS_TP
Event ID	2004
Event name	vRtrMplsTpLspPtTypeMismatchClear
SNMP notification prefix and OID	TIMETRA-MPLS-TP-MIB.vRtrMplsTpNotifications.4
Default severity	minor
Source stream	main
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

46.5 vRtrMplsTpLspRevertMismatchAlarm

Table 978: 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
Source stream	main

Property name	Value
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

46.6 vRtrMplsTpLspRevertMismatchClear

Table 979: 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
Source stream	main
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

47 MSDP

47.1 msdpBackwardTransition

Table 980: 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
Source stream	main
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

47.2 msdpEstablished

Table 981: msdpEstablished properties

Property name	Value
Application name	MSDP
Event ID	2001
Event name	msdpEstablished

Property name	Value
SNMP notification prefix and OID	MSDP-MIB.msdpTraps.1
Default severity	minor
Source stream	main
Message format string	MSDP FSM for peer *$strPeer$* has entered ESTABLISHED state.
Cause	The MSDP FSM entered the ESTABLISHED state.
Effect	N/A
Recovery	N/A

47.3 tmnxMsdpNgActSrcLimExcd

Table 982: 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
Source stream	main
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

47.4 tmnxMsdpNgGroupSrcActMsgsExcd

Table 983: 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
Source stream	main
Message format string	Active source limit *$tmnxMsdpNgPeerGroupMaxActSources$* reached for group *$strGrpPref$*. Num exceeded *$tmnxMsdpNgPeerGroupAct MsgsExMax$*
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

47.5 tmnxMsdpNgPeerActSrcLimExcd

Table 984: 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
Source stream	main
Message format string	Active source limit *$strLimit$* for peer *$strPeer$* has been exceeded.Num exceeded *$tmnxMsdpNgPeerStatsActSrcLimExcd$*.

Property name	Value
Cause	The tmnxMsdpNgPeerActSrcLimExcd event is generated whenever the active source limit has been exceeded for the peer.
Effect	N/A
Recovery	N/A

47.6 tmnxMsdpNgRPFFailure

Table 985: tmnxMsdpNgRPFFailure properties

Property name	Value
Application name	MSDP
Event ID	2010
Event name	tmnxMsdpNgRPFFailure
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.3
Default severity	minor
Source stream	main
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

47.7 tmnxMsdpNgSourceSrcActMsgsExcd

Table 986: tmnxMsdpNgSourceSrcActMsgsExcd properties

Property name	Value
Application name	MSDP

Property name	Value
Event ID	2011
Event name	tmnxMsdpNgSourceSrcActMsgsExcd
SNMP notification prefix and OID	TIMETRA-MSDP-NG-MIB.tmnxMsdpNgNotifications.4
Default severity	minor
Source stream	main
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

48 NAT

48.1 tmnxNatDetAddrMapOperStateChngd

Table 987: tmnxNatDetAddrMapOperStateChngd properties

Property name	Value
Application name	NAT
Event ID	2047
Event name	tmnxNatDetAddrMapOperStateChngd
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.47
Default severity	minor
Source stream	main
Message format string	The state of deterministic address-map inside range *$tmnxNatDetAddrMapInStart$* to *$tmnxNatDetAddrMapInEnd$* type *$tmnxNatDetAddrMapSubType$* nat-policy ' *$tmnxNatDetAddrMapNatPolicy$*' changed to *$tmnxNatDetAddrMapOperState$ - $tmnxNatNotifyDescription$*
Cause	The cause is explained in the tmnxNatNotifyDescription.
Effect	While the operational state is down, subscribers matching the address-map cannot use deterministic NAT; if configured so, they can fall back on another NAT policy.
Recovery	The recovery action depends on the cause.

48.2 tmnxNatDetMap2OperStateChanged

Table 988: tmnxNatDetMap2OperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2042

Property name	Value
Event name	tmnxNatDetMap2OperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.42
Default severity	minor
Source stream	main
Message format string	The state of deterministic prefix-map map *$tmnxNatDetPfxMapAddr$*/*$tmnxNatDetPfxMapAddrPrefixLength$* type *$tmnxNatDetPfxMapSubType$* nat-policy '*$tmnxNatDetPfxMapNatPolicy$*' start *$tmnxNatDetMap2InStart$* end *$tmnxNatDetMap2InEnd$* changed to *$tmnxNatDetMap2OperState$* - *$tmnxNatNotifyDescription$*
Cause	The cause is explained in the tmnxNatNotifyDescription.
Effect	While the operational state is down, subscribers matching the prefix cannot use deterministic NAT; if configured so, they can fall back on another NAT policy.
Recovery	The recovery action depends on the cause.

48.3 tmnxNatDetPfxMapOperStateChanged

Table 989: tmnxNatDetPfxMapOperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2041
Event name	tmnxNatDetPfxMapOperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.41
Default severity	minor
Source stream	main
Message format string	The state of deterministic prefix-map *$tmnxNatDetPfxMapAddr$*/*$tmnxNatDetPfxMapAddrPrefixLength$* type *$tmnxNatDetPfxMapSubType$* nat-policy '*$tmnxNatDetPfxMapNatPolicy$*' changed to *$tmnxNatDetPfxMapOperState$* - *$tmnxNatNotifyDescription$*
Cause	The cause is explained in the tmnxNatNotifyDescription.

Property name	Value
Effect	While the operational state is down, subscribers matching the prefix cannot use deterministic NAT; if configured so, they can fall back on another NAT policy.
Recovery	The recovery action depends on the cause.

48.4 tmnxNatDetPlcyChanged

Table 990: 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
Source stream	main
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.

48.5 tmnxNatDynamicConfigMismatch

Table 991: tmnxNatDynamicConfigMismatch properties

Property name	Value
Application name	NAT

Property name	Value
Event ID	2043
Event name	tmnxNatDynamicConfigMismatch
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.43
Default severity	warning
Source stream	main
Message format string	The system cannot dynamically install the destination prefix *$tmnx NatNotifyInsideAddr$/ $tmnxNatNotifyInsideAddrPrefixLen$* imported from the outside router instance *$tmnxNatNotifyOutsideVRtrID$* and associated with the NAT policy *$tmnxNatNotifyName$* in the inside router instance *$tmnxNatNotifyInsideVRtrID$*: *$tmnxNatNotify Description$*
Cause	The cause is explained in the tmnxNatNotifyDescription.
Effect	The destination-prefix is not imported.
Recovery	The recovery action logically follows from the specified cause.

48.6 tmnxNatFwd2EntryAdded

Table 992: tmnxNatFwd2EntryAdded properties

Property name	Value
Application name	NAT
Event ID	2031
Event name	tmnxNatFwd2EntryAdded
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.31
Default severity	minor
Source stream	main
Message format string	{*$tmnxNatNotifyPISeqNum$*} *$tmnxNatNotifyTruthValue$ $tmnxNat Fwd2OutAddr$* [*$tmnxNatFwd2OutPort$*] -- 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

Property name	Value
	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.

48.7 tmnxNatFwd2OperStateChanged

Table 993: 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
Source stream	main
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-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.

48.8 tmnxNatInAddrPrefixBlksFree

Table 994: 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
Source stream	main
Message format string	Possible messages: • {*$tmnxNatNotifyPlSeqNum$*} all blocks freed of all subscribers type *$tmnxNatNotifySubscriberType$* in inside router instance *$tmnxNatNotifyInsideVRtrID$* address type *$tmnxNatNotifyInsideAddrType$* prefix *$tmnxNatNotifyInsideAddr$*/*$tmnxNatNotifyInsideAddrPrefixLen$* MDA *$tmnxNatNotifyMdaCardSlotNum$*/*$tmnxNatNotifyMdaSlotNum$* ESA-VM *$tmnxNatNotifyIsaMemberEsaNum$*/ *$tmnxNatNotifyIsaMemberEsaVappNum$* at *$tmnxNatNotifyDateAndTime$* - *$tmnxNatNotifyDescription$* • {*$tmnxNatNotifyPlSeqNum$*} all blocks freed of all subscribers type *$tmnxNatNotifySubscriberType$* with NAT policy index *$tmnxNatNotifyPolicyIndex$* in inside router instance *$tmnxNatNotifyInsideVRtrID$* address type *$tmnxNatNotifyInsideAddrType$* prefix *$tmnxNatNotifyInsideAddr$*/*$tmnxNatNotifyInsideAddrPrefixLen$* MDA *$tmnxNatNotifyMdaCardSlotNum$*/ *$tmnxNatNotifyMdaSlotNum$* ESA-VM *$tmnxNatNotifyIsaMemberEsaNum$*/*$tmnxNatNotifyIsaMemberEsaVappNum$* 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

Property name	Value
	type. The values of tmnxNatNotifyMdaChassisIndex, tmnxNatNotify MdaCardSlotNum and tmnxNatNotifyMdaSlotNum identify the ISA MDA where the blocks were processed. All notifications of this type are sequentially numbered with the tmnxNatNotifyPlSeqNum. The value of tmnxNatNotifyPolicyIndex is the numerical identifier of the NAT policy used for this allocation; it can be used for correlation with the tmnx NatPlBlockAllocationLsn notification; the value zero means that this notification can be correlated with all the tmnxNatPlBlockAllocation Lsn notifications of the subscriber. This type of notification is typically the consequence of one or more configuration changes; the nature of these changes is indicated in the tmnxNatNotifyDescription.
Effect	N/A
Recovery	N/A

48.9 tmnxNatIsaGrpIsDegraded

Table 995: 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
Source stream	main
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

48.10 tmnxNatIsaGrpOperStateChanged

Table 996: tmnxNatIsaGrpOperStateChanged properties

Property name	Value
Application name	NAT
Event ID	2024
Event name	tmnxNatIsaGrpOperStateChanged
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.24
Default severity	minor
Source stream	main
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

48.11 tmnxNatIsaMemberSessionUsageHigh

Table 997: 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
Source stream	main

Property name	Value
Message format string	The session usage high water status changed to *$tmnxNatIsaMemberSessionUsageHi$*. (EsaNum *$tmnxNatIsaMemberEsaNum$*, EsaVapp Num *$tmnxNatIsaMemberEsaVappNum$*)
Cause	N/A
Effect	N/A
Recovery	N/A

48.12 tmnxNatL2AwSubIcmpPortUsageHigh

Table 998: tmnxNatL2AwSubIcmpPortUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2007
Event name	tmnxNatL2AwSubIcmpPortUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.7
Default severity	warning
Source stream	main
Message format string	The ICMP port usage high water status changed to *$tmnxNatL2AwSubStatIcmpPortUsageH$* for subscriber *$tmnxSubInfoSubIdent$* using policy *$tmnxNatL2AwSubStatNatPolicy$*
Cause	N/A
Effect	N/A
Recovery	N/A

48.13 tmnxNatL2AwSubSessionUsageHigh

Table 999: 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
Source stream	main
Message format string	The session usage high water status changed to *$tmnxNatL2AwSubStatSessionUsageHi$* for subscriber *$tmnxSubInfoSubIdent$* using policy *$tmnxNatL2AwSubStatNatPolicy$*
Cause	N/A
Effect	N/A
Recovery	N/A

48.14 tmnxNatL2AwSubTcpPortUsageHigh

Table 1000: tmnxNatL2AwSubTcpPortUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2009
Event name	tmnxNatL2AwSubTcpPortUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.9
Default severity	warning
Source stream	main
Message format string	The TCP port usage high water status changed to *$tmnxNatL2AwSubStatTcpPortUsageHi$* for subscriber *$tmnxSubInfoSubIdent$* using policy *$tmnxNatL2AwSubStatNatPolicy$*
Cause	N/A

Property name	Value
Effect	N/A
Recovery	N/A

48.15 tmnxNatL2AwSubUdpPortUsageHigh

Table 1001: 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
Source stream	main
Message format string	The UDP port usage high water status changed to *$tmnxNatL2AwSubStatUdpPortUsageHi$* for subscriber *$tmnxSubInfoSubIdent$* using policy *$tmnxNatL2AwSubStatNatPolicy$*
Cause	N/A
Effect	N/A
Recovery	N/A

48.16 tmnxNatLsnSubBlksFree

Table 1002: tmnxNatLsnSubBlksFree properties

Property name	Value
Application name	NAT
Event ID	2021
Event name	tmnxNatLsnSubBlksFree

Property name	Value
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.21
Default severity	minor
Source stream	main
Message format string	{*$tmnxNatNotifyPlSeqNum$*} LSN subscriber all blocks freed *$tmnxNatNotifyLsnSubId$ $tmnxNatNotifySubscriberType$ %$tmnxNatNotifyNumber$ $tmnxNatNotifyInsideVRtrID$ $tmnxNatNotifyInsideAddr$* MDA *$tmnxNatNotifyMdaCardSlotNum$*/*$tmnxNatNotifyMdaSlotNum$* ESA-VM *$tmnxNatNotifyIsaMemberEsaNum$*/*$tmnxNatNotifyIsaMemberEsaVappNum$* 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

48.17 tmnxNatLsnSubIcmpPortUsgHigh

Table 1003: 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
Source stream	main

Property name	Value
Message format string	The ICMP port usage high water status changed to *$tmnxNatQryLsnSubResIcmpPortUsgHi$* for host *$tmnxNatNotifyInsideAddr$* in router *$tmnxNatNotifyInsideVRtrID$* policy
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

48.18 tmnxNatLsnSubSessionUsgHigh

Table 1004: 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
Source stream	main
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

Property name	Value
Recovery	N/A

48.19 tmnxNatLsnSubTcpPortUsgHigh

Table 1005: 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
Source stream	main
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

48.20 tmnxNatLsnSubUdpPortUsgHigh

Table 1006: tmnxNatLsnSubUdpPortUsgHigh properties

Property name	Value
Application name	NAT

Property name	Value
Event ID	2027
Event name	tmnxNatLsnSubUdpPortUsgHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.27
Default severity	warning
Source stream	main
Message format string	The UDP port usage high water status changed to *$tmnxNatQryLsnSubResUdpPortUsgHi$* for host *$tmnxNatNotifyInsideAddr$* in router *$tmnxNatNotifyInsideVRtrID$* policy
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

48.21 tmnxNatMapRuleChange

Table 1007: 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
Source stream	main
Message format string	map-t map-domain *$tmnxNatMapDomName$* mapping-rule *$tmnxNatMapRuleName$* rule-prefix=*$tmnxNatMapRulePrefix$*/ *$tmnxNatMapRulePrefixLength$* ipv4-prefix=*$tmnxNatMapRuleIpv4Prefix$*/*$tmnxNatMapRuleIpv4PrefixLength$* ea-length= *$tmnxNatMapRuleEaLength$*

Property name	Value
	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.

48.22 tmnxNatMaxNbrSubsOrHostsExceeded

Table 1008: tmnxNatMaxNbrSubsOrHostsExceeded properties

Property name	Value
Application name	NAT
Event ID	2037
Event name	tmnxNatMaxNbrSubsOrHostsExceeded
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.37
Default severity	minor
Source stream	main
Message format string	The maximum number of *$tmnxNatNotifyMemberSubOrHostDesc$* on the group ISA member has been exceeded at *$tmnxNatNotifyDateAndTime$*. (group *$tmnxNatNotifyIsaGrpId$* - member *$tmnxNatNotifyIsaMemberId$* - chassis *$tmnxNatNotifyMdaChassisIndex$* - MDA *$tmnxNatNotifyMdaCardSlotNum$*/*$tmnxNatNotifyMdaSlotNum$* - ESA-VM *$tmnxNatNotifyIsaMemberEsaNum$*/*$tmnxNatNotifyIsaMemberEsaVappNum$*)
Cause	The tmnxNatMaxNbrSubsOrHostsExceeded notification is sent when the maximum number of LSN/DSM/L2aware subscribers or L2aware hosts on the member of the MDA has been exceeded.

Property name	Value
Effect	The system can't process additional subscribers/hosts of that type on that member.
Recovery	Additional ISA hardware or an upgrade of ISA's should to be considered.

48.23 tmnxNatMdaActive

Table 1009: 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
Source stream	main
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

48.24 tmnxNatMdaDetectsLoadSharingErr

Table 1010: tmnxNatMdaDetectsLoadSharingErr properties

Property name	Value
Application name	NAT

Property name	Value
Event ID	2023
Event name	tmnxNatMdaDetectsLoadSharingErr
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.23
Default severity	minor
Source stream	main
Message format string	The NAT MDA *$tmnxCardSlotNum$*/*$tmnxMDASlotNum$* in group *$tmnxNatIsaGrpId$* has detected load sharing errors and has dropped *$tmnxNatNotifyCounter$* more packets.
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.

48.25 tmnxNatNbrSubsOrHostsBelowThrsh

Table 1011: tmnxNatNbrSubsOrHostsBelowThrsh properties

Property name	Value
Application name	NAT
Event ID	2038
Event name	tmnxNatNbrSubsOrHostsBelowThrsh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.38
Default severity	minor
Source stream	main
Message format string	The number of *$tmnxNatNotifyMemberSubOrHostDesc$* on the group ISA member dropped below the threshold of 95% at *$tmnxNatNotifyDateAndTime$*. (group *$tmnxNatNotifyIsaGrpId$* - member *$tmnxNatNotifyIsaMemberId$* - chassis *$tmnxNatNotifyMdaChassisIndex$* - MDA *$tmnxNatNotifyMdaCardSlotNum$*/*$tmnxNatNotifyMdaSlotNum$* - ESA-VM *$tmnxNatNotifyIsaMemberEsaNum$*/*$tmnxNatNotifyIsaMemberEsaVappNum$*)

Property name	Value
Cause	The tmnxNatNbrSubsOrHostsBelowThrsh notification is sent when the number of LSN/DSM/L2aware subscribers or L2aware hosts dropped below the threshold of 95%.
Effect	The system can process again additional subscribers/hosts of that type on that member.
Recovery	There is no recovery required for this notification.

48.26 tmnxNatPcpSrvStateChanged

Table 1012: 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
Source stream	main
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.

48.27 tmnxNatPlAddrFree

Table 1013: tmnxNatPlAddrFree properties

Property name	Value
Application name	NAT
Event ID	2016
Event name	tmnxNatPlAddrFree
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.16
Default severity	minor
Source stream	main
Message format string	{*$tmnxNatNotifyPlSeqNum$*} Free [*$tmnxNatNotifyOutsideAddr$* - *$tmnxNatNotifyOutsideEndAddr$*] -- inside *$insideVRtrIDName$* at *$tmnxNatNotifyDateAndTime$* - *$tmnxNatNotifyDescription$*
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

48.28 tmnxNatPlBlockAllocationL2Aw

Table 1014: tmnxNatPlBlockAllocationL2Aw properties

Property name	Value
Application name	NAT
Event ID	2013
Event name	tmnxNatPlBlockAllocationL2Aw

Property name	Value
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.13
Default severity	minor
Source stream	main
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 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

48.29 tmnxNatPlBlockAllocationLsn

Table 1015: 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
Source stream	main
Message format string	{*$tmnxNatNotifyPlSeqNum$*} Map *$tmnxNatNotifyTruthValue$ $tmnx NatNotifyOutsideAddr$* [*$tmnxNatNotifyPort$-$tmnxNatNotifyPort2$*] MDA *$tmnxNatNotifyMdaCardSlotNum$*/*$tmnxNatNotifyMdaSlotNum*

Property name	Value
	$* ESA-VM *$tmnxNatNotifyIsaMemberEsaNum$/$tmnxNatNotifyIsaMemberEsaVappNum$
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 tmnxNatNotifyPort 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 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 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 tmnxNatPlAddrFree summary event, that may indicate this number in the tmnxNatNotifyDescription object. 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

48.30 tmnxNatPlL2AwBlockUsageHigh

Table 1016: 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
Source stream	main

Property name	Value
Message format string	The block usage high water status changed to *$tmnxNatPlBlockUsageHi$*.
Cause	N/A
Effect	N/A
Recovery	N/A

48.31 tmnxNatPlL2AwMembrBlockUsageHigh

Table 1017: tmnxNatPlL2AwMembrBlockUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2044
Event name	tmnxNatPlL2AwMembrBlockUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.44
Default severity	warning
Source stream	main
Message format string	The subscriber usage high water status changed to *$tmnxNatPlL2AwSubscrUsageHi$* for pool *$tmnxNatPlName$* on ISA group *$tmnxNatIsaGrpId$* member *$tmnxNatIsaMemberId$* MDA chassis *$tmnxNatIsaMemberMdaChassisIndex$* card slot *$tmnxNatIsaMemberMdaCardSlotNum$* slot *$tmnxNatIsaMemberMdaSlotNum$* ESA-VM *$tmnxNatIsaMemberEsaNum$/ $tmnxNatIsaMemberEsaVappNum$*
Cause	The tmnxNatPlL2AwMembrBlockUsageHigh notification is sent when the subscriber usage of an L2-Aware NAT address pool reaches its high watermark ('true') or when it reaches its low watermark again ('false') on a particular member MDA of its ISA group.
Effect	N/A
Recovery	N/A

48.32 tmnxNatPlLsnMemberBlockUsageHigh

Table 1018: 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
Source stream	main
Message format string	The block usage high water status changed to *$tmnxNatPlLsnMemberBlockUsageHi$* for pool *$tmnxNatPlName$* on ISA group *$tmnxNatIsaGrpId$* member *$tmnxNatIsaMemberId$* MDA *$tmnxNatIsaMemberMdaCardSlotNum$*/ *$tmnxNatIsaMemberMdaSlotNum$* ESA-VM *$tmnxNatIsaMemberEsaNum$*/*$tmnxNatIsaMemberEsaVappNum$*
Cause	N/A
Effect	N/A
Recovery	N/A

48.33 tmnxNatPlLsnMemberPortUsageHigh

Table 1019: tmnxNatPlLsnMemberPortUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2046
Event name	tmnxNatPlLsnMemberPortUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.46
Default severity	warning

Property name	Value
Source stream	main
Message format string	Possible messages: • The port usage high water status changed to *$tmnxNatNotifyPlLsnMbrPortUsageHi$* for router *$vRtrID$* pool *$tmnxNatNotifyPoolName$* protocol *$tmnxNatNotifyPlLsnMbrProtocol$* on ISA group *$tmnxNatIsaGrpId$* member *$tmnxNatIsaMemberId$* MDA chassis *$tmnxNatIsaMemberMdaChassisIndex$* card slot *$tmnxNatIsaMemberMdaCardSlotNum$* slot *$tmnxNatIsaMemberMdaSlotNum$* ESA-VM *$tmnxNatIsaMemberEsaNum$*/*$tmnxNatIsaMemberEsaVappNum$* • The port usage high water status changed to *$tmnxNatNotifyPlLsnMbrPortUsageHi$* for router *$vRtrID$* pool *$tmnxNatNotifyPoolName$* protocol *$tmnxNatNotifyPlLsnMbrProtocol$* on ISA group *$tmnxNatIsaGrpId$* member *$tmnxNatIsaMemberId$* MDA chassis *$tmnxNatIsaMemberMdaChassisIndex$* card slot *$tmnxNatIsaMemberMdaCardSlotNum$* slot *$tmnxNatIsaMemberMdaSlotNum$* ESA-VM *$tmnxNatIsaMemberEsaNum$*/*$tmnxNatIsaMemberEsaVappNum$* Outside address *$tmnxNatNotifyOutsideAddr$*
Cause	The tmnxNatPlLsnMemberPortUsageHigh notification is sent when the port usage of an LSN pool with flexible port allocation reaches its high or low watermark.
Effect	N/A
Recovery	N/A

48.34 tmnxNatPlLsnRedActiveChanged

Table 1020: 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
Source stream	main

Property name	Value
Message format string	The Large Scale NAT activity changed to *$tmnxNatPlLsnRedActive$* for pool *$tmnxNatPlName$ - $tmnxNatNotifyDescription$*
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 tmnx NatVrtrInRedPeerAddr 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 tmnxNatPlLsn RedExpPrefix 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.

48.35 tmnxNatPlMemberExtBlockUsageHigh

Table 1021: tmnxNatPlMemberExtBlockUsageHigh properties

Property name	Value
Application name	NAT
Event ID	2045
Event name	tmnxNatPlMemberExtBlockUsageHigh
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.45
Default severity	warning
Source stream	main
Message format string	The extended port block usage high water status changed to *$tmnx NatNotifyMbrExPrtBlckUsageHi$* for router *$vRtrID$* pool *$tmnxNat NotifyPoolName$* on ISA group *$tmnxNatIsaGrpId$* member *$tmnx*

Property name	Value
	NatIsaMemberId$* MDA chassis *$tmnxNatIsaMemberMdaChassis Index$* card slot *$tmnxNatIsaMemberMdaCardSlotNum$* slot *$tmnx NatIsaMemberMdaSlotNum$* ESA-VM *$tmnxNatIsaMemberEsaNum$/ $tmnxNatIsaMemberEsaVappNum$ Outside address *$tmnxNatNotify OutsideIPv4Addr$*
Cause	The tmnxNatPlMemberExtBlockUsageHigh notification is sent when the extended port block usage of a NAT address pool reaches its high watermark ('true') or when it reaches its low watermark again ('false') on a particular member MDA of its ISA group.
Effect	N/A
Recovery	N/A

48.36 tmnxNatResourceProblemCause

Table 1022: 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
Source stream	main
Message format string	*$tmnxNatNotifyDescription$*
Cause	N/A
Effect	N/A
Recovery	N/A

48.37 tmnxNatResourceProblemDetected

Table 1023: 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
Source stream	main
Message format string	The status of the NAT resource problem indication changed to *$tmnx NatResourceProblem$*.
Cause	N/A
Effect	N/A
Recovery	N/A

48.38 tmnxNatVappActive

Table 1024: tmnxNatVappActive properties

Property name	Value
Application name	NAT
Event ID	2039
Event name	tmnxNatVappActive
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.39
Default severity	minor
Source stream	main
Message format string	The Virtual NAT Application *$tmnxNatEsaNum$*/*$tmnxNatEsaVapp Num$* is now *$tmnxNatNotifyTruthValue$* in group *$tmnxNatIsaGrpId$* .
Cause	The tmnxNatVappActive notification is sent when the value of the object tmnxNatVappStatOperState changes from 'primary' to any other value,

Property name	Value
	or the other way around. The value 'primary' means that the Virtual NAT Application is active in the group.
Effect	N/A
Recovery	N/A

48.39 tmnxNatVappDetectsLoadSharingErr

Table 1025: tmnxNatVappDetectsLoadSharingErr properties

Property name	Value
Application name	NAT
Event ID	2040
Event name	tmnxNatVappDetectsLoadSharingErr
SNMP notification prefix and OID	TIMETRA-NAT-MIB.tmnxNatNotifications.40
Default severity	minor
Source stream	main
Message format string	The Virtual NAT Application *$tmnxNatEsaNum$*/*$tmnxNatEsaVapp Num$* in group *$tmnxNatIsaGrpId$* has detected load sharing errors and has dropped *$tmnxNatNotifyCounter$* more packets.
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 Virtual NAT Application drops all incorrectly load-balanced traffic.
Recovery	Upgrade the ingress IOM, or change the configuration.

48.40 tmnxNatVrtrOutDnatOnlyRoutesHigh

Table 1026: 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
Source stream	main
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.

49 NTP

49.1 tmnxNtpAuthMismatch

Table 1027: 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
Source stream	main
Message format string	NTP message is received with an *$tmnxNtpAuthKeyFailType$* from *$tmnxNtpPeersPeerAddress$* in *$tmnxNtpPeersPeerVRtrID$*
Cause	The tmnxNtpAuthMismatch notification is generated when tmnxNtp AuthCheck has a value of true and an NTP message is received with an incorrect authentication key, key id, or key type. tmnxNtpPeersPeer AddrType and tmnxNtpPeersPeerAddress indicate the Internet address of the peer that sent the message that failed authentication. The value of tmnxNtpPeersPeerVRtrID indicates the virtual router ID of the ntp peer.
Effect	N/A
Recovery	N/A

49.2 tmnxNtpNoServersAvail

Table 1028: 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
Source stream	main
Message format string	No NTP servers are available.
Cause	No NTP servers are available.
Effect	N/A
Recovery	N/A

49.3 tmnxNtpOperChange

Table 1029: 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
Source stream	main
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

49.4 tmnxNtpServerChange

Table 1030: 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
Source stream	main
Message format string	NTP server has changed: Old server *$strOldServer$* in *$intOldVRtrId$*, New server *$tmnxNtpPeersPeerAddress$* in *$tmnxNtpPeersPeerVRtrID$*
Cause	The tmnxNtpServerChange notification is generated when more than one NTP servers are configured in a system and a different NTP server is selected because the operational status of the earlier NTP server has changed. The value of tmnxNtpPeersPeerAddress indicates the address of the new NTP server. The value of tmnxNtpPeersPeerVRtrID indicates the virtual router ID of the new NTP server.
Effect	A new NTP server was selected.
Recovery	N/A

49.5 tmnxNtpServersAvail

Table 1031: tmnxNtpServersAvail properties

Property name	Value
Application name	NTP
Event ID	2003
Event name	tmnxNtpServersAvail
SNMP notification prefix and OID	TIMETRA-NTP-MIB.tmnxNtpNotifications.3

Property name	Value
Default severity	minor
Source stream	main
Message format string	NTP servers are available.
Cause	NTP servers are now available.
Effect	N/A
Recovery	N/A

50 OAM

50.1 svcIdInvalid

Table 1032: svcIdInvalid properties

Property name	Value
Application name	OAM
Event ID	2053
Event name	svcIdInvalid
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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

50.2 svcIdWrongType

Table 1033: svcIdWrongType properties

Property name	Value
Application name	OAM
Event ID	2054
Event name	svcIdWrongType
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	minor
Source stream	main
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

50.3 tmnxAncpLoopbackTestCompleted

Table 1034: 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
Default severity	warning
Source stream	main
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 explicitly requested.
Effect	N/A
Recovery	N/A

50.4 tmnxAncpLoopbackTestCompletedL

Table 1035: tmnxAncpLoopbackTestCompletedL properties

Property name	Value
Application name	OAM
Event ID	2005
Event name	tmnxAncpLoopbackTestCompletedL
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
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

50.5 tmnxOamDiagTestCompleted

Table 1036: tmnxOamDiagTestCompleted properties

Property name	Value
Application name	OAM
Event ID	2150
Event name	tmnxOamDiagTestCompleted
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamDiagNotifications.1
Default severity	minor
Source stream	main
Message format string	OAM *$tmnxOamDiagCtlTestMode$* test " *$tmnxOamDiagCtlTestIndex$*" created by "*$tmnxOamDiagCtlOwnerIndex$*" run #*$tmnxOamTestRunIndex$* completed

Property name	Value
Cause	A tmnxOamDiagTestCompleted trap is generated at the end of every diagnostic test run. A diagnostic test is configured using tmnxOam DiagCtlTable. tmnxOamDiagCtlTestMode indicates the type of the diagnostic test (e.g. 'findEgressDiag(1)'). tmnxOamTestRunIndex indicates the run number of the completed diagnostic test run. For example, the second run of a test with owner 'owner_A' and test 'test_Z' has tmnxOamTestRunIndex=2.
Effect	The result of the test run can be read (e.g. from the indicated row in tmnxOamFindEgrDiagResultsTable).
Recovery	No recovery is required.

50.6 tmnxOamLdpTtraceAutoDiscState

Table 1037: 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
Source stream	main
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

50.7 tmnxOamLdpTtraceFecDisStatus

Table 1038: 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
Source stream	main
Message format string	The FEC *$strTmnxOamLTtraceFecPrefix$*/*$strTmnxOamLTtraceFecPrefLen$* 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
Recovery	N/A

50.8 tmnxOamLdpTtraceFecPFailUpdate

Table 1039: 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
Source stream	main
Message format string	Path probe state update for the 'auto discovered' FEC, *$strTmnxOamLTtraceFecPrefix$*/ *$strTmnxOamLTtraceFecPrefLen$*. *$tmnx*

Property name	Value
	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

50.9 tmnxOamLdpTtraceFecProbeState

Table 1040: 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
Source stream	main
Message format string	The probe state of the 'auto discovered' FEC, *$strTmnxOamLTtrace FecPrefix$/ $strTmnxOamLTtraceFecPrefLen$*, has changed to *$tmnx OamLTtraceFecProbeState$.$tmnxOamLTtraceFecFailedProbes$* 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

50.10 tmnxOamPingProbeFailedV3

Table 1041: 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
Source stream	main
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

50.11 tmnxOamPingTestCompletedV3

Table 1042: tmnxOamPingTestCompletedV3 properties

Property name	Value
Application name	OAM
Event ID	2003
Event name	tmnxOamPingTestCompletedV3
SNMP notification prefix and OID	TIMETRA-OAM-TEST-MIB.tmnxOamPingNotifications.10
Default severity	minor
Source stream	main

Property name	Value
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

50.12 tmnxOamPingTestFailedV3

Table 1043: 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
Source stream	main
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

50.13 tmnxOamPmThrClear

Table 1044: 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
Source stream	main
Message format string	OAM-PM TCA cleared 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$*, bin lower bound (us) *$tmnxOamPmNotifThr BinLowerBound$*, configured threshold *$tmnxOamPmNotifThrCfg Clear$*, operational value *$tmnxOamPmNotifThrOperClear$*. TCA type *$tmnxOamPmNotifThrStateType$*, suspect flag *$tmnxOamPmStsBase Suspect$*.
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.

50.14 tmnxOamPmThrRaise

Table 1045: tmnxOamPmThrRaise properties

Property name	Value
Application name	OAM
Event ID	2300
Event name	tmnxOamPmThrRaise
SNMP notification prefix and OID	TIMETRA-OAM-PM-MIB.tmnxOamPmNotifications.1
Default severity	warning
Source stream	main
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.

Property name	Value
Recovery	Fix the cause of the excessive loss or excessive delay.

50.15 tmnxOamSaaThreshold

Table 1046: 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
Source stream	main
Message format string	OAM SAA *$tmnxOamSaaCtlTestMode$* test "*$tmnxOamSaaCtlTest Index$*" created by "*$tmnxOamSaaCtlOwnerIndex$*" run # *$tmnxOam SaaTTestRunIndex$* crossed *$tmnxOamSaaTDirection$ $tmnxOam SaaTType$* threshold *$tmnxOamSaaTThreshold$* with value *$tmnx OamSaaTValue$*
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

50.16 tmnxOamSathSvcStrmCompleted

Table 1047: tmnxOamSathSvcStrmCompleted properties

Property name	Value
Application name	OAM
Event ID	2401

Property name	Value
Event name	tmnxOamSathSvcStrmCompleted
SNMP notification prefix and OID	TIMETRA-OAM-SERV-ACTIV-TEST-MIB.tmnxOamSathNotifications.2
Default severity	warning
Source stream	main
Message format string	Service activation service test "*$tmnxOamSathCfgSvcTestName$*" run *$tmnxOamSathStsSvcTestRun$* service stream *$tmnxOamSathCfgSvcStrmNum$* completed (*$tmnxOamSathStsSvcStrmOprState$*)
Cause	The tmnxOamSathSvcStrmCompleted notification is sent at the end of a Y.1564 service-stream run.
Effect	Informational. If the service-stream run failed, a live deployment of the services owned by the service-stream may fail.
Recovery	If the service-stream run failed, investigate the cause.

50.17 tmnxOamSathSvcTestCompleted

Table 1048: tmnxOamSathSvcTestCompleted properties

Property name	Value
Application name	OAM
Event ID	2400
Event name	tmnxOamSathSvcTestCompleted
SNMP notification prefix and OID	TIMETRA-OAM-SERV-ACTIV-TEST-MIB.tmnxOamSathNotifications.1
Default severity	warning
Source stream	main
Message format string	Service activation service test "*$tmnxOamSathCfgSvcTestName$*" run *$tmnxOamSathStsSvcTestRun$* completed (*$tmnxOamSathStsSvcTestOprState$*)
Cause	The tmnxOamSathSvcTestCompleted notification is sent at the end of a Y.1564 service-test run.
Effect	Informational. If the service-test run failed, a live deployment of the services owned by the service-test may fail.

Property name	Value
Recovery	If the service-test run failed, investigate the cause.

50.18 tmnxOamTrPathChange

Table 1049: 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
Source stream	main
Message format string	OAM *$tmnxOamTrCtlTestMode$* test "*$tmnxOamTrCtlTestIndex$*" created by " *$tmnxOamTrCtlOwnerIndex$*" run *#$tmnxOamTrResults TestRunIndex$* path changed
Cause	The path to a target has changed.
Effect	N/A
Recovery	N/A

50.19 tmnxOamTrTestCompleted

Table 1050: 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

Property name	Value
Default severity	minor
Source stream	main
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

50.20 tmnxOamTrTestFailed

Table 1051: 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
Source stream	main
Message format string	OAM *$tmnxOamTrCtlTestMode$* test "*$tmnxOamTrCtlTestIndex$*" created by " *$tmnxOamTrCtlOwnerIndex$*" run #*$tmnxOamTrResults TestRunIndex$* failed
Cause	The OAM trace route test failed to complete successfully.
Effect	N/A
Recovery	N/A

50.21 tmnxTwampRflInactivityTimeout

Table 1052: tmnxTwampRflInactivityTimeout properties

Property name	Value
Application name	OAM
Event ID	2205
Event name	tmnxTwampRflInactivityTimeout
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.6
Default severity	minor
Source stream	main
Message format string	TWAMP Reflector test session localAddr *$tmnxTwampRflNotifLocalAddr$* port *$tmnxTwampRflNotifLocalUdpPort$* remoteAddr *$tmnxTwampRflNotifRemoteAddr$* port *$tmnxTwampRflNotifRemoteUdpPort$* disconnected because REFWAIT expired, Client Connection Addr *$tmnxTwampSrvNotifClientAddr$*
Cause	The tmnxTwampRflInactivityTimeout notification is generated when a TWAMP test session is disconnected by the TWAMP Reflector because the session was inactive for a period exceeding the reflector's inactivity timeout (tmnxTwampRflInactTimeout).
Effect	The TWAMP reflector cannot receive any traffic on the disconnected session.
Recovery	Check the IP connectivity between this reflector and the TWAMP client.

50.22 tmnxTwampSrvInactivityTimeout

Table 1053: 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
Source stream	main

Property name	Value
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.

50.23 tmnxTwampSrvMaxConnsExceeded

Table 1054: tmnxTwampSrvMaxConnsExceeded properties

Property name	Value
Application name	OAM
Event ID	2201
Event name	tmnxTwampSrvMaxConnsExceeded
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.2
Default severity	minor
Source stream	main
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.

Property name	Value
Recovery	Configure the system-level maximum number of concurrent TWAMP control connections to a larger value, or disconnect any TWAMP control connection.

50.24 tmnxTwampSrvMaxSessExceeded

Table 1055: 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
Source stream	main
Message format string	TWAMP server session to client *$tmnxTwampSrvNotifClientAddr$* could not be established because the system limit (*$tmnxTwampSrv SessionCount$* 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.
Recovery	Configure the system-level maximum number of concurrent TWAMP sessions to a larger value, or disconnect any TWAMP session.

50.25 tmnxTwampSrvPfxMaxConnsExceeded

Table 1056: tmnxTwampSrvPfxMaxConnsExceeded properties

Property name	Value
Application name	OAM

Property name	Value
Event ID	2202
Event name	tmnxTwampSrvPfxMaxConnsExceeded
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.3
Default severity	minor
Source stream	main
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.

50.26 tmnxTwampSrvPfxMaxSessExceeded

Table 1057: tmnxTwampSrvPfxMaxSessExceeded properties

Property name	Value
Application name	OAM
Event ID	2204
Event name	tmnxTwampSrvPfxMaxSessExceeded
SNMP notification prefix and OID	TIMETRA-TWAMP-MIB.tmnxTwampNotifications.5
Default severity	minor
Source stream	main
Message format string	TWAMP server session to client *$tmnxTwampSrvNotifClientAddr$* could not be established because the limit for prefix *$tmnxTwampSrv*

Property name	Value
	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.

51 OPEN_FLOW

51.1 tmnxOFFlowEntryInsertFailed

Table 1058: 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
Source stream	main
Message format string	Failed to add flow-entry for open-flow switch " *$tmnxOFSwitchName$*" flow-table *$tmnxOFFlowTableId$*. Flow-table Oper Status: *$tmnxOFFlowTableOperStatus$*. Failure Reason *$tmnxOFNotifyDescription$*
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.

52 OSPF

52.1 tmnxOspfAdjBfdSessionSetupFail

Table 1059: 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
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: BFD session setup failed with reason *$tmnxOspfBfdSessSetupFailReason$*
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.

52.2 tmnxOspfAreaMaxAgeLsa

Table 1060: tmnxOspfAreaMaxAgeLsa properties

Property name	Value
Application name	OSPF
Event ID	2013
Event name	tmnxOspfAreaMaxAgeLsa

Property name	Value
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.13
Default severity	warning
Source stream	main
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

52.3 tmnxOspfAreaOriginateLsa

Table 1061: 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
Source stream	main
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

52.4 tmnxOspfAsMaxAgeLsa

Table 1062: 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
Source stream	main
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

52.5 tmnxOspfAsOriginateLsa

Table 1063: 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
Source stream	main

Property name	Value
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.
Effect	N/A
Recovery	N/A

52.6 tmnxOspfDynHostnameDuplicate

Table 1064: tmnxOspfDynHostnameDuplicate properties

Property name	Value
Application name	OSPF
Event ID	2061
Event name	tmnxOspfDynHostnameDuplicate
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.61
Default severity	warning
Source stream	main
Message format string	Duplicate advertising of *$tmnxOspfHostnameName$*
Cause	The tmnxOspfDynHostnameDuplicate notification is sent when another system advertises the same hostname as the local router.
Effect	No effect.
Recovery	No recovery is necessary.

52.7 tmnxOspfDynHostnameInconsistent

Table 1065: tmnxOspfDynHostnameInconsistent properties

Property name	Value
Application name	OSPF
Event ID	2062
Event name	tmnxOspfDynHostnameInconsistent
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.62
Default severity	warning
Source stream	main
Message format string	Inconsistent advertising of *$tmnxOspfHostnameName$*
Cause	The tmnxOspfDynHostnameInconsistent notification is sent when there are inconsistencies for and advertised hostname.
Effect	No effect.
Recovery	No recovery is necessary.

52.8 tmnxOspfExportLimitReached

Table 1066: 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
Source stream	main
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.

Property name	Value
Recovery	Change OSPF export policy.

52.9 tmnxOspfExportLimitWarning

Table 1067: 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
Source stream	main
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

52.10 tmnxOspfFailureDisabled

Table 1068: tmnxOspfFailureDisabled properties

Property name	Value
Application name	OSPF
Event ID	2038
Event name	tmnxOspfFailureDisabled

Property name	Value
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.38
Default severity	warning
Source stream	main
Message format string	LCL_RTR_ID *$tmnxOspfRouterId$*: OSPF disabled. Reason: *$tmnx OspfFailureReasonCode$*
Cause	A tmnxOspfFailureDisabled notification is generated when OSPF is operationally brought down due to an operational problem. Reason for the failure is indicated by tmnxOspfFailureReasonCode.
Effect	OSPF is going in shutdown.
Recovery	After 30 seconds, OSPF will autonomously start up. If the operational problem is still there then it will shutdown again.

52.11 tmnxOspfFaOperParticipationDown

Table 1069: tmnxOspfFaOperParticipationDown properties

Property name	Value
Application name	OSPF
Event ID	2063
Event name	tmnxOspfFaOperParticipationDown
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.63
Default severity	warning
Source stream	main
Message format string	The oper-participation of *$tmnxOspfFlexAlgoId$* in area *$tmnxOspf AreaId$* is operationally down due to *$tmnxOspfNotifyDescription$*.
Cause	The tmnxOspfFaOperParticipationDown notification is sent when the Flexible Algorithm Participation is operationally down. This notification occurs each time when: a) there are no Flexible Algorithm Definitions(FADs) present for the Flexible Algorithm. b) the FAD chosen for Flex-Algo calculation has unsupported parameters like unsupported: 1. Metric-Type 2. Calculation-Type 3. Constraint 4. Fad-Flags 5. Sub-Tlv

Property name	Value
Effect	The node will cease to participate in that Flexible Algorithm, and won't advertise its participation in SR-algo sub-TLV.
Recovery	The operator may make sure if at least one FAD is present for that Flexible Algorithm, and in case of unsupported FAD, correct the FAD parameters to send supported values from remote side.

52.12 tmnxOspfLsdbApproachingOverflow

Table 1070: tmnxOspfLsdbApproachingOverflow properties

Property name	Value
Application name	OSPF
Event ID	2015
Event name	tmnxOspfLsdbApproachingOverflow
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.15
Default severity	warning
Source stream	main
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

52.13 tmnxOspfLsdbOverflow

Table 1071: tmnxOspfLsdbOverflow properties

Property name	Value
Application name	OSPF

Property name	Value
Event ID	2014
Event name	tmnxOspfLsdbOverflow
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.14
Default severity	warning
Source stream	main
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

52.14 tmnxOspfNgIfAuthFailure

Table 1072: tmnxOspfNgIfAuthFailure properties

Property name	Value
Application name	OSPF
Event ID	2044
Event name	tmnxOspfNgIfAuthFailure
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.44
Default severity	warning
Source stream	main
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

Property name	Value
Recovery	N/A

52.15 tmnxOspfNgIfConfigError

Table 1073: 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
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Conflicting configuration *$tmnxOspfConfigErrorType$* on interface *$ospfIfIpAddress$* from *$tmnxOspfPacketSrcAddress$* 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

52.16 tmnxOspfNgIfRxBadPacket

Table 1074: tmnxOspfNgIfRxBadPacket properties

Property name	Value
Application name	OSPF
Event ID	2045

Property name	Value
Event name	tmnxOspfNgIfRxBadPacket
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.45
Default severity	warning
Source stream	main
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

52.17 tmnxOspfNgIfStateChange

Table 1075: 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
Source stream	main
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).
Effect	N/A
Recovery	N/A

52.18 tmnxOspfNgLdpSyncExit

Table 1076: 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
Source stream	main
Message format string	IGP-LDP synchronization has stopped for interface *$vRtrIfIndex$* because *$strReason$*.
Cause	When IGP-LDP synchronization is configured on an interface then the interface is initially announced with maximum metric in the router LSA. This notification is sent when IGP-LDP synchronization finishes, that is when tmnxOspfNgIfLdpSyncTimerState changes to a state higher than timerActive.
Effect	The IGP link metric is restored to normal level.
Recovery	N/A

52.19 tmnxOspfNgLdpSyncTimerStarted

Table 1077: 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

Property name	Value
Source stream	main
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

52.20 tmnxOspfNgLinkMaxAgeLsa

Table 1078: tmnxOspfNgLinkMaxAgeLsa properties

Property name	Value
Application name	OSPF
Event ID	2050
Event name	tmnxOspfNgLinkMaxAgeLsa
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.50
Default severity	warning
Source stream	main
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

52.21 tmnxOspfNgLinkOriginateLsa

Table 1079: 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
Source stream	main
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

52.22 tmnxOspfNgNbrRestartHlprStsChg

Table 1080: 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
Source stream	main

Property name	Value
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Helper status for neighbor *$ospf NbrIpAddr$* router *$ospfNbrRtrId$* changed to *$tmnxOspfNgNbrRestart HelperStatus$* (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

52.23 tmnxOspfNgNbrStateChange

Table 1081: 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
Source stream	main
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 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

52.24 tmnxOspfNgNbrStrictBfdBlocked

Table 1082: tmnxOspfNgNbrStrictBfdBlocked properties

Property name	Value
Application name	OSPF
Event ID	2064
Event name	tmnxOspfNgNbrStrictBfdBlocked
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.64
Default severity	warning
Source stream	main
Message format string	BFD strict-mode capable neighbor *$tmnxOspfNgNbrRtrId$* is blocked
Cause	The tmnxOspfNgNbrStrictBfdBlocked notification is sent when, with BFD strict-mode enabled, OSPF has received a Hello packet from a BFD strict-mode capable neighbor but will not list that neighbor in the Hello packet sent on that interface while waiting for BFD session setup completion. This should be an edge-triggered notification. We should not send a second notification about Hellos received from or sent to the same source.
Effect	No effect.
Recovery	No recovery is necessary.

52.25 tmnxOspfNssaTranslatorStatusChg

Table 1083: 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

Property name	Value
Default severity	warning
Source stream	main
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

52.26 tmnxOspfOverloadEntered

Table 1084: tmnxOspfOverloadEntered properties

Property name	Value
Application name	OSPF
Event ID	2023
Event name	tmnxOspfOverloadEntered
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.23
Default severity	warning
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Overload entered (event *$tmnxOspfLastOverloadEnterCode$*) *$tmnxOspfNotifyDescription$*
Cause	OSPF entered the overload state. vRtrOspfLastOverloadEnterCode holds the condition which caused OSPF to get into overload.
Effect	N/A
Recovery	N/A

52.27 tmnxOspfOverloadExited

Table 1085: 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
Source stream	main
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

52.28 tmnxOspfOverloadWarning

Table 1086: 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
Source stream	main

Property name	Value
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Reached overload limit (event *$tmnxOspfLastOverloadEnterCode$*) *$tmnxOspfNotifyDescription$*
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

52.29 tmnxOspfRejectedAdjacencySet

Table 1087: tmnxOspfRejectedAdjacencySet properties

Property name	Value
Application name	OSPF
Event ID	2059
Event name	tmnxOspfRejectedAdjacencySet
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.59
Default severity	warning
Source stream	main
Message format string	Rejected adjacency set *$tmnxOspfNotifyDescription$*
Cause	The tmnxOspfRejectedAdjacencySet notification is sent when an adjacency can not be assigned to an adjacency-set because it does not terminate on the same neighbor node as the other adjacencies. This notification each time the adjacency-set is programmed.
Effect	Adjacency-set nhops will not include this adjacency.
Recovery	Remove the interface from the adjacency-set or change the adjacency-set type to non parallel.

52.30 tmnxOspfRejectedAdjacencySid

Table 1088: 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
Source stream	main
Message format string	LCL_RTR_ID *$tmnxOspfRouterId$*: *$tmnxOspfNotifyDescription$*
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 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.

52.31 tmnxOspfRestartStatusChange

Table 1089: 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
Source stream	main

Property name	Value
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

52.32 tmnxOspfRoutesExpLmtDropped

Table 1090: tmnxOspfRoutesExpLmtDropped properties

Property name	Value
Application name	OSPF
Event ID	2041
Event name	tmnxOspfRoutesExpLmtDropped
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.41
Default severity	warning
Source stream	main
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

52.33 tmnxOspfShamIfAuthFailure

Table 1091: 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
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Packet failed *$tmnxOspfConfigErrorType$* authentication from sham-link neighbor *$tmnxOspfShamIfRemoteNbrAddress$* in *$tmnxOspfPacketType$*
Cause	A tmnxOspfShamIfAuthFailure notification is generated when a packet has been received on a sham link from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
Effect	The packet is discarded.
Recovery	Correct authentication configuration in this router or in the other router.

52.34 tmnxOspfShamIfConfigError

Table 1092: 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
Source stream	main

Property name	Value
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Conflicting configuration *$tmnxOspfConfigErrorType$* from sham-link neighbor *$tmnxOspfShamIfRemoteNbrAddress$* in *$tmnxOspfPacketType$*
Cause	A tmnxOspfShamIfConfigError notification is generated when a packet has been received on a sham link from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event 'optionMismatch' should cause a notification only if it prevents an adjacency from forming.
Effect	No OSPF adjacency is formed.
Recovery	Correct conflicting OSPF configuration parameters.

52.35 tmnxOspfShamIfRxBadPacket

Table 1093: 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
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: Bad packet, *$tmnxOspfBadPacketErrType$*, received from sham-link neighbor *$tmnxOspfShamIfRemoteNbrAddress$* in *$tmnxOspfPacketType$*
Cause	A tmnxOspfShamIfRxBadPacket notification is generated when an OSPF packet that cannot be parsed has been received on a sham link.
Effect	The OSPF packet is dropped.
Recovery	Resolve root cause why packet could not be parsed by OSPF. The necessary action depends on tmnxOspfBadPacketErrType.

52.36 tmnxOspfShamIfStateChange

Table 1094: 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
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*:State of sham-link interface *$tmnxOspfShamIfIndex$* with neighbor *$tmnxOspfShamIfRemoteNbrAddress$* changed to *$tmnxOspfShamIfState$*
Cause	A tmnxOspfShamIfStateChange notification is generated when there has been a change in the state of an OSPF sham link. This notification should be 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	The state of an OSPF sham link changed.
Recovery	Investigate why the state changed if it was not intentional.

52.37 tmnxOspfShamNbrRestartHlprStsChg

Table 1095: 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

Property name	Value
Default severity	warning
Source stream	main
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	An tmnxOspfShamNbrRestartHlprStsChg notification is generated when there has been a change in the graceful restart helper state for the sham link neighbor. This notification should be generated when the sham link neighbor restart helper status transitions for a sham link neighbor.
Effect	Notifies a change in the graceful restart helper state for the sham link neighbor.
Recovery	N/A

52.38 tmnxOspfShamNbrStateChange

Table 1096: 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
Source stream	main
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: State of sham-link neighbor *$tmnxOspfShamNbrRtrId$* changed to *$tmnxOspfShamNbrState$*
Cause	A tmnxOspfShamNbrStateChange notification is generated when there has been a change in the state of an OSPF sham link neighbor. This notification should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).

Property name	Value
Effect	There has been a change in the state of an OSPF sham link neighbor.
Recovery	N/A

52.39 tmnxOspfSidStatsIndexAlloc

Table 1097: tmnxOspfSidStatsIndexAlloc properties

Property name	Value
Application name	OSPF
Event ID	2060
Event name	tmnxOspfSidStatsIndexAlloc
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.60
Default severity	warning
Source stream	main
Message format string	Possible messages: • Statistics Index Allocation status changed to *$tmnxOspfNotifStatsIndexStatus$* for adjacency-set *$tmnxOspfSidStatsAdjSet$* • Statistics Index Allocation status changed to *$tmnxOspfNotifStatsIndexStatus$* for adjacency interface *$tmnxOspfSidStatsIfIndex$* • Statistics Index Allocation status changed to *$tmnxOspfNotifStatsIndexStatus$* for node *$tmnxOspfSidStatsPrefix$*/*$tmnxOspfSidStatsPrefixLength$*
Cause	The tmnxOspfSidStatsIndexAlloc notification is sent when the system is not able to allocate a statistic index to at least one SID. This indication is sent once, i.e. if the system retries to allocate a stat index but fails no new notification is sent. Conversely, in case the system resolves the situation and allocates stat indices to all needed SIDs a notification is sent to indicate that stat allocation is in nominal state.
Effect	No effect.
Recovery	No recovery is necessary.

52.40 tmnxOspfSpfRunsRestarted

Table 1098: 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
Source stream	main
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

52.41 tmnxOspfSpfRunsStopped

Table 1099: 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
Source stream	main

Property name	Value
Message format string	LCL_RTR_ID *$ospfRouterIdIpAddr$*: SPF runs stopped - insufficient memory resources
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.

52.42 tmnxOspfSrgbBadLabelRange

Table 1100: 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
Source stream	main
Message format string	LCL_RTR_ID *$tmnxOspfRouterId$*: Bad SRGB label range from router *$tmnxOspfNotifSrgbAdvRtrID$* in area *$tmnxOspfNotifSrgbAreaId$*: startLabel:*$tmnxOspfNotifSrgbRangeStartLbl$* maxIdx: *$tmnxOspfNotifSrgbRangeMaxIdx$* will be ignored
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.

52.43 tmnxOspfSrSidError

Table 1101: tmnxOspfSrSidError properties

Property name	Value
Application name	OSPF
Event ID	2053
Event name	tmnxOspfSrSidError
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.53
Default severity	minor
Source stream	main
Message format string	SID label error: SID *$tmnxOspfSrPfxSid$*, area *$tmnxOspfSrPfxArea Id$*, algo *$tmnxOspfSrPfxSidAlgorithm$*, reason: *$tmnxOspfNotify Description$*
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.

52.44 tmnxOspfSrSidNotInLabelRange

Table 1102: 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
Source stream	main

Property name	Value
Message format string	Possible messages: • SID not in range of router *$tmnxOspfNotifPfxNhAdvRtr$*: SID *$tmnxOspfSrPfxSid$*, area *$tmnxOspfSrPfxAreaId$*, algo *$tmnxOspfSrPfxSidAlgorithm$*, NO LABEL RANGE defined • SID not in range of router *$tmnxOspfNotifPfxNhAdvRtr$*: SID *$tmnxOspfSrPfxSid$*, area *$tmnxOspfSrPfxAreaId$*, algo *$tmnxOspfSrPfxSidAlgorithm$*, startLbl *$tmnxOspfNotifPfxSidRangeStartLbl$*, max Idx *$tmnxOspfNotifPfxSidRangeMaxIdx$*
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.

52.45 tmnxOspfVirtIfAuthFailure

Table 1103: 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
Source stream	main
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

Property name	Value
Recovery	N/A

52.46 tmnxOspfVirtIfConfigError

Table 1104: 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
Source stream	main
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 parameters. Note that the event optionMismatch should generate an event only if it prevents an adjacency from forming.
Effect	N/A
Recovery	N/A

52.47 tmnxOspfVirtIfRxBadPacket

Table 1105: tmnxOspfVirtIfRxBadPacket properties

Property name	Value
Application name	OSPF
Event ID	2009

Property name	Value
Event name	tmnxOspfVirtIfRxBadPacket
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.9
Default severity	warning
Source stream	main
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

52.48 tmnxOspfVirtIfStateChange

Table 1106: 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
Default severity	warning
Source stream	main
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

Property name	Value
Recovery	N/A

52.49 tmnxOspfVirtNbrRestartHlprStsChg

Table 1107: 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
Source stream	main
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

52.50 tmnxOspfVirtNbrStateChange

Table 1108: tmnxOspfVirtNbrStateChange properties

Property name	Value
Application name	OSPF
Event ID	2003

Property name	Value
Event name	tmnxOspfVirtNbrStateChange
SNMP notification prefix and OID	TIMETRA-OSPF-NG-MIB.tmnxOspfNotifications.3
Default severity	warning
Source stream	main
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 Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).
Effect	N/A
Recovery	N/A

53 PCAP

53.1 tmnxPcapBufferFull

Table 1109: 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
Source stream	main
Message format string	Session *$tmnxPcapSessionName$*'s allocated buffer is full, with size *$tmnxPcapSessionBufferSize$*. Total number of packets dropped by this session is *$tmnxPcapSessionDroppedPackets$* packets.
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.

53.2 tmnxPcapBufferReadWriteFailure

Table 1110: tmnxPcapBufferReadWriteFailure properties

Property name	Value
Application name	PCAP
Event ID	2003

Property name	Value
Event name	tmnxPcapBufferReadWriteFailure
SNMP notification prefix and OID	TIMETRA-PCAP-MIB.tmnxPcapNofitications.3
Default severity	major
Source stream	main
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.

53.3 tmnxPcapFileError

Table 1111: 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
Source stream	main
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.

Property name	Value
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.

53.4 tmnxPcapSoftwareFailure

Table 1112: 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
Source stream	main
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.

54 PCEP

54.1 tmnxPcepPccPeerStateChange

Table 1113: tmnxPcepPccPeerStateChange properties

Property name	Value
Application name	PCEP
Event ID	2001
Event name	tmnxPcepPccPeerStateChange
SNMP notification prefix and OID	TIMETRA-PCEP-MIB.tmnxPcepNotifyPrefix.1
Default severity	minor
Source stream	main
Message format string	PCC peer *$tmnxPcepPccPeerAddr$* state changed to *$tmnxPcepPccPeerOperState$*
Cause	This notification is generated when the specified PCC Peer changes operational state.
Effect	The PCC peer changes state to operationally up or down.
Recovery	Appropriate investigation or action can be taken.

55 PFCP

55.1 tmnxPfcpInvalidIe

Table 1114: tmnxPfcpInvalidIe properties

Property name	Value
Application name	PFCP
Event ID	2001
Event name	tmnxPfcpInvalidIe
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.56
Default severity	warning
Source stream	main
Message format string	Invalid IE ignored in PFCP request for session *$tmnxPfcpSeIdHigh$*: *$tmnxPfcpSeIdLow$*: *$tmnxSubAdditionalInfo$*
Cause	The system receives a PFCP request containing an Information Element that it considers invalid but still continues processing the rest of the request. The reason why the IE is considered invalid is given in the object tmnxSubAdditionalInfo.
Effect	The system may still set up the PFCP session but without some of the requested properties.
Recovery	Recovery, if any, depends on the cause.

55.2 tmnxPfcpNoSecondaryInterface

Table 1115: tmnxPfcpNoSecondaryInterface properties

Property name	Value
Application name	PFCP
Event ID	2003

Property name	Value
Event name	tmnxPfcpNoSecondaryInterface
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.58
Default severity	warning
Source stream	main
Message format string	The secondary GTP interface in network instance *$tmnxPfcpVRtrID $* that is indicated in a PFCP request for session *$tmnxPfcpSeIdHigh $*:*$tmnxPfcpSeIdLow$* does not exist: *$tmnxSubAdditionalInfo$*
Cause	The system receives a PFCP request containing a Traffic Endpoint Information Element with a Network Instance that refers to the secondary GTP interface and this system has no secondary GTP interface configured.
Effect	The system will still set up the PFCP session but using the primary GTP interface.
Recovery	In the network instance indicated by 'tmnxPfcpVRtrID', configure the secondary GTP interface with the object 'TIMETRA-WLAN-GW-MIB::tmnxGtpUpfDataEndptSecItfName'.

55.3 tmnxPfcpNoSuchCalltraceProfile

Table 1116: tmnxPfcpNoSuchCalltraceProfile properties

Property name	Value
Application name	PFCP
Event ID	2002
Event name	tmnxPfcpNoSuchCalltraceProfile
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.57
Default severity	warning
Source stream	main
Message format string	Unknown calltrace trace-profile *$tmnxSubNotifName$* in PFCP request for session *$tmnxPfcpSeIdHigh$*:*$tmnxPfcpSeIdLow$*: *$tmnxSub AdditionalInfo$*
Cause	The system receives a PFCP request containing an Information Element that refers to a call-trace trace-profile while there is no such

Property name	Value
	trace-profile present in the system configuration but a default trace-profile is configured for the PFCP association. There is a mismatch between the operation of the Control Plane (CP) and the call-trace configuration in this User Plane (UP) system.
Effect	The system performs call tracing for the session but uses a default trace-profile rather than the requested one.
Recovery	Remove the mismatch between the operation of the Control Plane (CP) and the call-trace configuration in this User Plane (UP) system.

56 PIM

56.1 vRtrPimNgBierInbInvBfrId

Table 1117: vRtrPimNgBierInbInvBfrId properties

Property name	Value
Application name	PIM
Event ID	2017
Event name	vRtrPimNgBierInbInvBfrId
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.17
Default severity	minor
Source stream	main
Message format string	bier inband JP with (*$vRtrPimNgNotifyBierInbSAddr$*, *$vRtrPim NgNotifyBierInbGAddr$*) from IBBR *$vRtrPimNgNotifyBierInbIAddr$* is dropped due to bfr-id mismatch, received bfr id *$vRtrPimNgNotifyBier InbInvBfrId$*.
Cause	The vRtrPimNgBierInbInvSD is generated when PIM receives a JP PDU with unsupported BFR id.
Effect	PIM will stop processing the Join/Prune PDU.
Recovery	The operator must ensure that downstream routers must have the bfr-id within 1..4096 range.

56.2 vRtrPimNgBierInbInvSD

Table 1118: vRtrPimNgBierInbInvSD properties

Property name	Value
Application name	PIM
Event ID	2016

Property name	Value
Event name	vRtrPimNgBierInbInvSD
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.16
Default severity	minor
Source stream	main
Message format string	bier inband JP with (*$vRtrPimNgNotifyBierInbSAddr$*, *$vRtrPim NgNotifyBierInbGAddr$*) from IBBR *$vRtrPimNgNotifyBierInbIAddr$* is dropped due to sub-domain mismatch, received sub domain id *$vRtr PimNgNotifyBierInbInvSDId$*.
Cause	The vRtrPimNgBierInbInvSD is generated when PIM receives a JP Pdu with unsupported sub-domain id.
Effect	PIM will stop processing the Join/Prune PDU.
Recovery	The operator must ensure that downstream routers must have the same sub-domain id.

56.3 vRtrPimNgBSRStateChange

Table 1119: 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
Source stream	main
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

56.4 vRtrPimNgDataMtReused

Table 1120: 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
Default severity	warning
Source stream	main
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

56.5 vRtrPimNgGrpInSSMRange

Table 1121: 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

Property name	Value
Source stream	main
Message format string	Received *$vRtrPimNgNotifyMsgType$* message on interface *$vRtr IfIndex$* 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

56.6 vRtrPimNgHelloDropped

Table 1122: 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
Source stream	main
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

56.7 vRtrPimNgIfMaxNbrReached

Table 1123: vRtrPimNgIfMaxNbrReached properties

Property name	Value
Application name	PIM
Event ID	2021
Event name	vRtrPimNgIfMaxNbrReached
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.21
Default severity	minor
Source stream	main
Message format string	Discarding hello on interface *$vRtrIfIndex$* as maximum of *$vRtrPim NgIfNbrCount$* pim interface neighbor limit is reached.
Cause	The vRtrPimNgIfMaxNbrReached is generated when the PIM interface has received more than 10K neighbors.
Effect	We restrict the number of neighbors to 10K in both per interface.
Recovery	The operated should be informed that the limit is higher than allowed.

56.8 vRtrPimNgIfNeighborLoss

Table 1124: 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
Source stream	main
Message format string	Lost adjacency with neighbor *$vRtrPimNgIfNeighborAddress$* on interface *$vRtrIfIndex$*
Cause	The PIM adjacency with a neighbor was lost.
Effect	N/A

Property name	Value
Recovery	N/A

56.9 vRtrPimNgIfNeighborUp

Table 1125: 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
Source stream	main
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

56.10 vRtrPimNgInstMaxNbrReached

Table 1126: vRtrPimNgInstMaxNbrReached properties

Property name	Value
Application name	PIM
Event ID	2020
Event name	vRtrPimNgInstMaxNbrReached
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.20

Property name	Value
Default severity	minor
Source stream	main
Message format string	Discarding Hello, maximum of *$vRtrPimNgInstNbrCount$* system pim neighbors reached.
Cause	The vRtrPimNgInstMaxNbrReached is generated when PIM instance has received more than 10K neighbors.
Effect	We restrict the number of neighbors to 10K per instance.
Recovery	The operator should be informed that that the limit is higher than allowed.

56.11 vRtrPimNgInvalidIPmsiTunnel

Table 1127: 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
Source stream	main
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 address specified by vRtrPimNgAFGenMdtDefGrpAddress. 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

Property name	Value
	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)'.

56.12 vRtrPimNgInvalidJoinPrune

Table 1128: 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
Source stream	main
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

56.13 vRtrPimNgInvalidRegister

Table 1129: 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
Source stream	main
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

56.14 vRtrPimNgMaxGraftRetry

Table 1130: vRtrPimNgMaxGraftRetry properties

Property name	Value
Application name	PIM
Event ID	2015

Property name	Value
Event name	vRtrPimNgMaxGraftRetry
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.15
Default severity	minor
Source stream	main
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.

56.15 vRtrPimNgMaxGrpsLimitExceeded

Table 1131: 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
Source stream	main
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 exceeded the maximum limit.
Effect	N/A
Recovery	N/A

56.16 vRtrPimNgMcacPlcyDropped

Table 1132: vRtrPimNgMcacPlcyDropped properties

Property name	Value
Application name	PIM
Event ID	2013
Event name	vRtrPimNgMcacPlcyDropped
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.13
Default severity	warning
Source stream	main
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

56.17 vRtrPimNgMDTLimitExceeded

Table 1133: 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
Source stream	main

Property name	Value
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

56.18 vRtrPimNgReplicationLmtExceeded

Table 1134: 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
Source stream	main
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

56.19 vRtrPimNgSGLimitExceeded

Table 1135: 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
Source stream	main
Message format string	Maximum number of multicast (S,G) records reached on IOM *$tmnx CardHwIndex$*, 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

56.20 vRtrPimNgUmhBMonFastFailPriToStb

Table 1136: vRtrPimNgUmhBMonFastFailPriToStb properties

Property name	Value
Application name	PIM
Event ID	2018
Event name	vRtrPimNgUmhBMonFastFailPriToStb
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.18
Default severity	minor
Source stream	main
Message format string	UMH bandwidth monitor based tunnel switch has happened at *$vRtrPimNgUmhBMonTimeStamp$* from the primary interface mpls-if- *$vRtrPimNgUmhBMonPrimaryIfIndex$* to the standby interface mpls-if-*$vRtrPimNgUmhBMonStandbyIfIndex$* when primary rate was *$v*

Property name	Value
	RtrPimNgUmhBMonPrimaryBW$* and standby rate was *$vRtrPim NgUmhBMonStandbyBW$.
Cause	The vRtrPimNgUmhBMonFastFailPriToStb is generated when there is a traffic switch in data-path.
Effect	Data-packets switches to the active path from primary to standby due to bandwidth delta.
Recovery	Recovery is based on revertive timer and traffic should switch back to primary tunnel automatically when the traffic recovers, else it remains on the standby tunnel.

56.21 vRtrPimNgUmhBMonFastFailStbToPri

Table 1137: vRtrPimNgUmhBMonFastFailStbToPri properties

Property name	Value
Application name	PIM
Event ID	2019
Event name	vRtrPimNgUmhBMonFastFailStbToPri
SNMP notification prefix and OID	TIMETRA-PIM-NG-MIB.vRtrPimNgNotifications.19
Default severity	minor
Source stream	main
Message format string	UMH bandwidth monitor based tunnel switch has happened at *$vRtr PimNgUmhBMonTimeStamp$* from the standby interface mpls-if- *$v RtrPimNgUmhBMonStandbyIfIndex$* to the primary interface mpls-if-*$vRtrPimNgUmhBMonPrimaryIfIndex$* when primary rate was *$v RtrPimNgUmhBMonPrimaryBW$* and standby rate was *$vRtrPim NgUmhBMonStandbyBW$*.
Cause	The vRtrPimNgUmhBMonFastFailStbToPri is generated when there is a traffic switch in data-path.
Effect	Data-packets switches to the active path from standby to primary due to bandwidth delta.
Recovery	Recovery is based on revertive timer and traffic should switch back to primary tunnel automatically when the traffic recovers, else it remains on the standby tunnel.

57 PIM_SNOOPING

57.1 tmnxPimSnpgIfMaxNbrReached

Table 1138: tmnxPimSnpgIfMaxNbrReached properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2005
Event name	tmnxPimSnpgIfMaxNbrReached
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.5
Default severity	minor
Source stream	main
Message format string	Discarding hello on pim service *$SvcId$* with SAP *$sapId$* as maximum of *$tmnxPimSnpgIntfNbrCount$* pim-snooping neighbor limit is reached.
Cause	The tmnxPimSnpgIfMaxNbrReached is generated when PIM snooping interface has received more than 10K neighbors.
Effect	We restrict the number of neighbors to 10K per interface.
Recovery	The operator should be informed that the limit is higher than allowed.

57.2 tmnxPimSnpgIfNeighborLoss

Table 1139: tmnxPimSnpgIfNeighborLoss properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2001
Event name	tmnxPimSnpgIfNeighborLoss

Property name	Value
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.1
Default severity	minor
Source stream	main
Message format string	Lost neighbor *$tmnxPimSnpgIfNbrAddress$* on *$ifName$*
Cause	The PIM adjacency with a neighbor was lost.
Effect	N/A
Recovery	N/A

57.3 tmnxPimSnpgIfNeighborUp

Table 1140: 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
Source stream	main
Message format string	Snooped new neighbor *$tmnxPimSnpgIfNbrAddress$* on *$ifName$*
Cause	The PIM adjacency with a new neighbor was established.
Effect	N/A
Recovery	N/A

57.4 tmnxPimSnpgMaxNbrReached

Table 1141: tmnxPimSnpgMaxNbrReached properties

Property name	Value
Application name	PIM_SNOOPING
Event ID	2006
Event name	tmnxPimSnpgMaxNbrReached
SNMP notification prefix and OID	TIMETRA-PIM-SNOOPING-MIB.tmnxPimSnpgNotifications.6
Default severity	minor
Source stream	main
Message format string	Discarding hello on pim service *$SvcId$* as maximum of *$tmnxPim SnpgNbrCount$* pim-snooping neighbor limit is reached.
Cause	The tmnxPimSnpgMaxNbrReached is generated when PIM snooping instance has received more than 10K neighbors.
Effect	We restrict the number of neighbors to 10K per instance.
Recovery	The operator should be informed that the limit is higher than allowed.

57.5 tmnxPimSnpgSGLimitExceeded

Table 1142: 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
Source stream	main
Message format string	Maximum number of multicast (S,G) records reached on IOM *$tmnx CardHwIndex$*, failed to program OIF record

Property name	Value
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

57.6 tmnxPimSnpgSnoopModeChanged

Table 1143: 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
Source stream	main
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

58 PORT

58.1 digitalDiagnosticMonitorCleared

Table 1144: digitalDiagnosticMonitorCleared properties

Property name	Value
Application name	PORT
Event ID	2041
Event name	digitalDiagnosticMonitorCleared
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.43
Default severity	minor
Source stream	main
Message format string	Possible messages: • SFF DDM (*$tmnxDDMFailedObject$*) cleared • SFF DDM Lane *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailed Object$*) cleared
Cause	Generated when an SFP/XFP that supports Digital Diagnostic Monitoring (DDM) clears a failed state.
Effect	N/A
Recovery	N/A

58.2 digitalDiagnosticMonitorFailed

Table 1145: digitalDiagnosticMonitorFailed properties

Property name	Value
Application name	PORT
Event ID	2030

Property name	Value
Event name	digitalDiagnosticMonitorFailed
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.35
Default severity	minor
Source stream	main
Message format string	Possible messages: • SFF DDM (*$tmnxDDMFailedObject$*) raised • SFF DDM Lane *$tmnxDDMLaneIdOrModule$* (*$tmnxDDMFailed Object$*) raised
Cause	Generated when an SFF that supports Digital Diagnostic Monitoring (DDM) enters a failed state.
Effect	N/A
Recovery	N/A

58.3 ds1AlarmClear

Table 1146: ds1AlarmClear properties

Property name	Value
Application name	PORT
Event ID	2016
Event name	ds1AlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.18
Default severity	minor
Source stream	main
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

58.4 ds1AlarmSet

Table 1147: ds1AlarmSet properties

Property name	Value
Application name	PORT
Event ID	2015
Event name	ds1AlarmSet
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.17
Default severity	minor
Source stream	main
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

58.5 ds1LoopbackStart

Table 1148: ds1LoopbackStart properties

Property name	Value
Application name	PORT
Event ID	2019
Event name	ds1LoopbackStart
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.24
Default severity	minor
Source stream	main
Message format string	DS1/E1 '*$tmnxDS1Loopback$*' Loopback Started

Property name	Value
Cause	The tmnxDS1E1LoopbackStarted notification is generated when a loopback is provisioned on a DS1/E1 port.
Effect	N/A
Recovery	N/A

58.6 ds1LoopbackStop

Table 1149: ds1LoopbackStop properties

Property name	Value
Application name	PORT
Event ID	2020
Event name	ds1LoopbackStop
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.25
Default severity	minor
Source stream	main
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

58.7 ds3AlarmClear

Table 1150: ds3AlarmClear properties

Property name	Value
Application name	PORT

Property name	Value
Event ID	2014
Event name	ds3AlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.16
Default severity	minor
Source stream	main
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

58.8 ds3AlarmSet

Table 1151: ds3AlarmSet properties

Property name	Value
Application name	PORT
Event ID	2013
Event name	ds3AlarmSet
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.15
Default severity	minor
Source stream	main
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
Recovery	N/A

58.9 ds3LoopbackStart

Table 1152: ds3LoopbackStart properties

Property name	Value
Application name	PORT
Event ID	2021
Event name	ds3LoopbackStart
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.26
Default severity	minor
Source stream	main
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
Recovery	N/A

58.10 ds3LoopbackStop

Table 1153: ds3LoopbackStop properties

Property name	Value
Application name	PORT
Event ID	2022
Event name	ds3LoopbackStop
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.27
Default severity	minor
Source stream	main
Message format string	DS3/E3 '*$tmnxDS3ChannelLoopback$*' Loopback Stopped

Property name	Value
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

58.11 dsxClockSyncStateChange

Table 1154: dsxClockSyncStateChange properties

Property name	Value
Application name	PORT
Event ID	2034
Event name	dsxClockSyncStateChange
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.37
Default severity	minor
Source stream	main
Message format string	Clock Sync State (*$tmnxDSXClockSyncStateObject$*)
Cause	Generated when the tmnxDS3ChannelClockSyncState changes for a DS3 or DS1 channel with adaptive or differential clock source.
Effect	N/A
Recovery	N/A

58.12 etherAlarmClear

Table 1155: etherAlarmClear properties

Property name	Value
Application name	PORT

Property name	Value
Event ID	2018
Event name	etherAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.23
Default severity	minor
Source stream	main
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

58.13 etherAlarmSet

Table 1156: etherAlarmSet properties

Property name	Value
Application name	PORT
Event ID	2017
Event name	etherAlarmSet
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.22
Default severity	minor
Source stream	main
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

58.14 etherDuplexNotCompatible

Table 1157: etherDuplexNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2028
Event name	etherDuplexNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.33
Default severity	major
Source stream	main
Message format string	Provisioned duplex *$tmnxPortEtherDuplex$* not compatible with MDA *$tmnxMdaNotifyType$*
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 duplex on an MDA port is not compatible with the inserted MDA.
Effect	N/A
Recovery	N/A

58.15 etherIngressRateCfgNotCompatible

Table 1158: etherIngressRateCfgNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2029
Event name	etherIngressRateCfgNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.34
Default severity	major

Property name	Value
Source stream	main
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
Recovery	N/A

58.16 etherLoopCleared

Table 1159: etherLoopCleared properties

Property name	Value
Application name	PORT
Event ID	2026
Event name	etherLoopCleared
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.31
Default severity	minor
Source stream	main
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

58.17 etherLoopDetected

Table 1160: etherLoopDetected properties

Property name	Value
Application name	PORT
Event ID	2025
Event name	etherLoopDetected
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.30
Default severity	minor
Source stream	main
Message format string	Ethernet loop detected on port *$tmnxPortNotifyPortId$*
Cause	The tmnxEqPortEtherLoopDetected notification is generated 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

58.18 etherSpeedNotCompatible

Table 1161: etherSpeedNotCompatible properties

Property name	Value
Application name	PORT
Event ID	2027
Event name	etherSpeedNotCompatible
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.32
Default severity	major
Source stream	main

Property name	Value
Message format string	Provisioned speed *$tmnxPortEtherSpeed$* not compatible with MDA *$tmnxMdaNotifyType$*
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

58.19 otuAlarms

Table 1162: otuAlarms properties

Property name	Value
Application name	PORT
Event ID	2037
Event name	otuAlarms
SNMP notification prefix and OID	TIMETRA-OTU-MIB.tmnxOtuNotifications.1
Default severity	minor
Source stream	main
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

58.20 portError

Table 1163: portError properties

Property name	Value
Application name	PORT
Event ID	2009
Event name	portError
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.14
Default severity	minor
Source stream	main
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

58.21 sdhLoopbackStart

Table 1164: sdhLoopbackStart properties

Property name	Value
Application name	PORT
Event ID	2023
Event name	sdhLoopbackStart
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.28
Default severity	minor
Source stream	main
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

Property name	Value
Recovery	N/A

58.22 sdhLoopbackStop

Table 1165: sdhLoopbackStop properties

Property name	Value
Application name	PORT
Event ID	2024
Event name	sdhLoopbackStop
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.29
Default severity	minor
Source stream	main
Message format string	Sonet/SDH '*$tmnxSonetLoopback$*' Loopback Stopped
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

58.23 SFPInserted

Table 1166: SFPInserted properties

Property name	Value
Application name	PORT
Event ID	2005
Event name	SFPInserted

Property name	Value
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.8
Default severity	minor
Source stream	main
Message format string	SFF Inserted
Cause	Generated when a SFP is inserted in the port.
Effect	N/A
Recovery	N/A

58.24 SFPRemoved

Table 1167: SFPRemoved properties

Property name	Value
Application name	PORT
Event ID	2006
Event name	SFPRemoved
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.9
Default severity	minor
Source stream	main
Message format string	SFF Removed
Cause	Generated when a SFP is removed from the port.
Effect	N/A
Recovery	N/A

58.25 SFPStatusBlocked

Table 1168: 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
Source stream	main
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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot 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.

58.26 SFPStatusCulprit

Table 1169: SFPStatusCulprit properties

Property name	Value
Application name	PORT
Event ID	2059
Event name	SFPStatusCulprit
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Source stream	main
Message format string	SFF culprit

Property name	Value
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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot 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.

58.27 SFPStatusDDMCorrupt

Table 1170: 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
Source stream	main
Message format string	SFF 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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot 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.

58.28 SFPStatusFailure

Table 1171: 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
Source stream	main
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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot 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.

58.29 SFPStatusInvalidFormFactor

Table 1172: SFPStatusInvalidFormFactor properties

Property name	Value
Application name	PORT
Event ID	2087
Event name	SFPStatusInvalidFormFactor
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36

Property name	Value
Default severity	minor
Source stream	main
Message format string	SFF In Invalid Form Factor State
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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot 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.

58.30 SFPStatusModuleFault

Table 1173: SFPStatusModuleFault properties

Property name	Value
Application name	PORT
Event ID	2088
Event name	SFPStatusModuleFault
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Source stream	main
Message format string	SFF In Fault State
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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot be used. The SFF and port will not recover without operator intervention.

Property name	Value
Recovery	Remove and re-insert the SFF device. If the problem persists then replace the SFF device.

58.31 SFPStatusOperational

Table 1174: 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
Source stream	main
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 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

58.32 SFPStatusReadError

Table 1175: SFPStatusReadError properties

Property name	Value
Application name	PORT
Event ID	2032

Property name	Value
Event name	SFPStatusReadError
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Source stream	main
Message format string	SFF 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 SR OS series systems.
Effect	The SFF device is not operational and the associated port cannot 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.

58.33 SFPStatusUnsupported

Table 1176: SFPStatusUnsupported properties

Property name	Value
Application name	PORT
Event ID	2033
Event name	SFPStatusUnsupported
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.36
Default severity	minor
Source stream	main
Message format string	SFF 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 SR OS series systems.

Property name	Value
Effect	The SFF device is not operational and the associated port cannot 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.

58.34 sonetSDHAlarmClear

Table 1177: sonetSDHAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2002
Event name	sonetSDHAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.5
Default severity	minor
Source stream	main
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

58.35 sonetSDHAlarmSet

Table 1178: sonetSDHAlarmSet properties

Property name	Value
Application name	PORT
Event ID	2001

Property name	Value
Event name	sonetSDHAlarmSet
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.4
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortNotifySonetAlarmReason$* Set
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

58.36 sonetSDHChannelAlarmClear

Table 1179: sonetSDHChannelAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2004
Event name	sonetSDHChannelAlarmClear
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.7
Default severity	minor
Source stream	main
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

58.37 sonetSDHChannelAlarmSet

Table 1180: sonetSDHChannelAlarmSet properties

Property name	Value
Application name	PORT
Event ID	2003
Event name	sonetSDHChannelAlarmSet
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.6
Default severity	minor
Source stream	main
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

58.38 tmnxCellPortCbsdAuthorized

Table 1181: tmnxCellPortCbsdAuthorized properties

Property name	Value
Application name	PORT
Event ID	2080
Event name	tmnxCellPortCbsdAuthorized
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.9
Default severity	minor
Source stream	main

Property name	Value
Message format string	CBSD *$tmnxPortPortID$* Authorized - CBSD Id: *$tmnxCellPortCbsd AuthId$*, Grant Id: *$tmnxCellPortCbsdAuthGrantId$*, Grant expire time: *$tmnxCellPortCbsdAuthGrantExpTime$*, Heartbeat interval: *$tmnxCell PortCbsdAuthHeartbeatInt$* seconds
Cause	The tmnxCellPortCbsdAuthorized notification is generated when the CBSD is authorized by the SAS.
Effect	The CBSD enables SR-OS on the cellular interface.
Recovery	Not applicable.

58.39 tmnxCellPortCbsdGranted

Table 1182: tmnxCellPortCbsdGranted properties

Property name	Value
Application name	PORT
Event ID	2079
Event name	tmnxCellPortCbsdGranted
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.8
Default severity	minor
Source stream	main
Message format string	CBSD *$tmnxPortPortID$* Granted - CBSD Id: *$tmnxCellPortCbsdAuth Id$*, Grant Id: *$tmnxCellPortCbsdAuthGrantId$*, Grant expire time: *$tmnxCellPortCbsdAuthGrantExpTime$*, Heartbeat interval: *$tmnxCell PortCbsdAuthHeartbeatInt$* seconds
Cause	The tmnxCellPortCbsdGranted notification is generated when the CBSD has received a grant Id from the SAS. The CBSD is not authorized until after the authorized notification is generated.
Effect	The CBSD is awaiting authorization from the SAS.
Recovery	Not applicable.

58.40 tmnxCellPortCbsdRegistered

Table 1183: tmnxCellPortCbsdRegistered properties

Property name	Value
Application name	PORT
Event ID	2077
Event name	tmnxCellPortCbsdRegistered
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.6
Default severity	minor
Source stream	main
Message format string	CBSD *$tmnxPortPortID$* Registered - CBSD Id: *$tmnxCellPortCbsdAuthId$*, Server: *$tmnxCellPortCbsdAuthCurSasSvrIp$*
Cause	The tmnxCellPortCbsdRegistered notification is generated when the CBSD successfully registers with the SAS.
Effect	After this notification is generated the CBSD continues the CBSD authorization procedures.
Recovery	Not applicable.

58.41 tmnxCellPortCbsdTransDown

Table 1184: tmnxCellPortCbsdTransDown properties

Property name	Value
Application name	PORT
Event ID	2081
Event name	tmnxCellPortCbsdTransDown
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.10
Default severity	minor
Source stream	main

Property name	Value
Message format string	CBSD *$tmnxPortPortID$* transitioned from *$tmnxCellCbsdAuthPrev TransState$* to *$tmnxCellCbsdAuthNewTransState$* - CBSD Id: *$tmnx CellPortCbsdAuthId$*, Grant Id: *$tmnxCellPortCbsdAuthGrantId$*, Reason: *$tmnxCellCbsdAuthFailReason$*, Response code: *$tmnxCell CbsdAuthRespCode$*
Cause	The tmnxCellPortCbsdTransDown notification is generated when the CBSD is transitioning to a lower state.
Effect	The CBSD proceeds to complete authorization with the SAS from the state the CBSD has transitioned to.
Recovery	Not applicable.

58.42 tmnxCellPortCbsdUnregistered

Table 1185: tmnxCellPortCbsdUnregistered properties

Property name	Value
Application name	PORT
Event ID	2078
Event name	tmnxCellPortCbsdUnregistered
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.7
Default severity	minor
Source stream	main
Message format string	CBSD *$tmnxPortPortID$* Unregistered - CBSD Id: *$tmnxCellPortCbsd AuthId$*, Reason: *$tmnxCellCbsdAuthFailReason$*, Response code: *$tmnxCellCbsdAuthRespCode$*
Cause	The tmnxCellPortCbsdUnregistered notification is generated when the CBSD is declared unregistered with the SAS.
Effect	The CBSD restarts the registration procedures with the SAS.
Recovery	Not applicable.

58.43 tmnxCellularActiveSimChange

Table 1186: tmnxCellularActiveSimChange properties

Property name	Value
Application name	PORT
Event ID	2070
Event name	tmnxCellularActiveSimChange
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.5
Default severity	major
Source stream	main
Message format string	Active SIM card switched to SIM *$tmnxCellMdaOperActiveSim$* (*$tmnxCellMdaSimLastSwitchReason$*)
Cause	The tmnxCellularActiveSimChange notification is generated when the active SIM card on the cellular MDA changes.
Effect	N/A
Recovery	N/A

58.44 tmnxCellularBearerCreated

Table 1187: tmnxCellularBearerCreated properties

Property name	Value
Application name	PORT
Event ID	2065
Event name	tmnxCellularBearerCreated
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.1
Default severity	warning
Source stream	main

Property name	Value
Message format string	Dedicated bearer id *$tmnxCellPortBearerId$* created on port *$tmnxPort PortID$*
Cause	The tmnxCellularBearerCreated notification is generated when the network creates a dedicated bearer on a cellular port.
Effect	N/A
Recovery	N/A

58.45 tmnxCellularBearerDeleted

Table 1188: tmnxCellularBearerDeleted properties

Property name	Value
Application name	PORT
Event ID	2066
Event name	tmnxCellularBearerDeleted
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.2
Default severity	warning
Source stream	main
Message format string	Dedicated bearer id *$tmnxCellPortBearerId$* deleted on port *$tmnxPort PortID$*
Cause	The tmnxCellularBearerDeleted notification is generated when the network removes a dedicated bearer on a cellular port.
Effect	N/A
Recovery	N/A

58.46 tmnxCellularBearerModified

Table 1189: tmnxCellularBearerModified properties

Property name	Value
Application name	PORT
Event ID	2067
Event name	tmnxCellularBearerModified
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.3
Default severity	warning
Source stream	main
Message format string	Bearer id *$tmnxCellPortBearerId$* modified on port *$tmnxPortPortID$*
Cause	The tmnxCellularBearerModified notification is generated when the network modifies a bearer on a cellular port.
Effect	N/A
Recovery	N/A

58.47 tmnxCellularNoServiceReset

Table 1190: tmnxCellularNoServiceReset properties

Property name	Value
Application name	PORT
Event ID	2069
Event name	tmnxCellularNoServiceReset
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.4
Default severity	critical
Source stream	main
Message format string	Could not establish service over the cellular port (*$tmnxCellMda NoServiceResetReason$*). Resetting the system in 60 seconds if this condition persists

Property name	Value
Cause	The tmnxCellularNoServiceReset notification is generated before the system resets because it could not establish service over the cellular interface.
Effect	The system will reset 60 seconds after this event is generated if it cannot establish service over the cellular interface.
Recovery	The reset of the system may cause the cellular port to become operational.

58.48 tmnxCellularRssiAlarm

Table 1191: tmnxCellularRssiAlarm properties

Property name	Value
Application name	PORT
Event ID	2085
Event name	tmnxCellularRssiAlarm
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.11
Default severity	minor
Source stream	main
Message format string	The RSSI level detected by cellular port *$tmnxPortNotifyPortId$* has been below the threshold *$tmnxCellSimCardRssiThresh$* dBm for the duration of *$tmnxCellSimCardRssiAlarmTime$* seconds
Cause	The tmnxCellularRssiAlarm notification is generated when the cellular port has detected the RSSI (Received Signal Strength Indicator) level fell below the configured minimum threshold tmnxCellSimCardRssi Thresh for a duration of time configured by tmnxCellSimCardRssiAlarm Time.
Effect	N/A.
Recovery	N/A.

58.49 tmnxCellularRssiAlarmClear

Table 1192: tmnxCellularRssiAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2086
Event name	tmnxCellularRssiAlarmClear
SNMP notification prefix and OID	TIMETRA-CELLULAR-MIB.tmnxCellularNotifications.12
Default severity	cleared
Source stream	main
Message format string	Alarm tmnxCellularRssiAlarm is cleared - The RSSI level detected by cellular port *$tmnxPortNotifyPortId$* has been equal to or above the threshold *$tmnxCellSimCardRssiThresh$* dBm for the duration of *$tmnxCellSimCardRssiAlarmTime$* seconds
Cause	After the tmnxCellularRssiAlarm is generated, the tmnxCellularRssi AlarmClear notification is generated when the cellular port has detected the RSSI (Received Signal Strength Indicator) level rose to equal or above the configured minimum threshold tmnxCellSimCardRssiThresh for the duration of time configured by tmnxCellSimCardRssiAlarmTime.
Effect	N/A.
Recovery	N/A.

58.50 tmnxDS0ChanGrpLoopbackStarted

Table 1193: tmnxDS0ChanGrpLoopbackStarted properties

Property name	Value
Application name	PORT
Event ID	2089
Event name	tmnxDS0ChanGrpLoopbackStarted
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.70
Default severity	major
Source stream	main

Property name	Value
Message format string	Started DS0ChanGrp '*$tmnxDS0ChanGroupLoopback$*' loopback on port *$tmnxPortNotifyPortId$*
Cause	The tmnxDS0ChanGrpLoopbackStarted notification is generated when a loopback is provisioned on a DS0 channel group. The value of tmnxDS0ChanGroupLoopback specifies the type of loopback that was configured.
Effect	Setting the DS0 channel group in loopback mode impacts the normal flow of traffic across the port.
Recovery	Remove loopback on the DS0 channel group to restore normal traffic flow.

58.51 tmnxDS0ChanGrpLoopbackStopped

Table 1194: tmnxDS0ChanGrpLoopbackStopped properties

Property name	Value
Application name	PORT
Event ID	2090
Event name	tmnxDS0ChanGrpLoopbackStopped
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.71
Default severity	major
Source stream	main
Message format string	Stopped DS0ChanGrp '*$tmnxDS0ChanGroupLoopback$*' loopback on port *$tmnxPortNotifyPortId$*
Cause	The tmnxDS0ChanGrpLoopbackStopped notification is generated when a loopback is removed on a DS0 channel group. The value of tmnxDS0ChanGroupLoopback specifies the type of loopback that was configured and has now been removed.
Effect	The loopback has been removed and normal traffic flow may resume.
Recovery	No recovery is required.

58.52 tmnxEqCohOptPortAlarm

Table 1195: 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
Source stream	main
Message format string	Coherent Optical Alarms Active: *$tmnxCohOptPortAlarmState$*
Cause	The tmnxEqCohOptPortAlarm 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. Note: The value of tmnxCohOptPortDefectPoints included in the notification may not reflect the latest data. A separate query of that object is required to view the latest data.
Effect	N/A
Recovery	N/A

58.53 tmnxEqPortEtherCrcAlarm

Table 1196: tmnxEqPortEtherCrcAlarm properties

Property name	Value
Application name	PORT
Event ID	2052
Event name	tmnxEqPortEtherCrcAlarm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.52

Property name	Value
Default severity	minor
Source stream	main
Message format string	CRC errors in excess of the configured *$tmnxPortNotifyEtherCrcAlarmValue$* threshold *$tmnxPortNotifyEtherCrcMultiplier$**10e-*$tmnxPortNotifyEtherCrcThreshold$* 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.

58.54 tmnxEqPortEtherCrcAlarmClear

Table 1197: 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
Source stream	main
Message format string	CRC errors in excess of the configured *$tmnxPortNotifyEtherCrcAlarmValue$* threshold *$tmnxPortNotifyEtherCrcMultiplier$**10e-*$tmnxPortNotifyEtherCrcThreshold$* Cleared
Cause	tmnxEqPortEtherCrcAlarmClear is generated when an Ethernet port CRC alarm condition is cleared or disabled.
Effect	N/A

Property name	Value
Recovery	N/A

58.55 tmnxEqPortEtherEgressRateChange

Table 1198: tmnxEqPortEtherEgressRateChange properties

Property name	Value
Application name	PORT
Event ID	2068
Event name	tmnxEqPortEtherEgressRateChange
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.62
Default severity	minor
Source stream	main
Message format string	Port *$tmnxNotifyPortId$* oper egress rate has changed to *$tmnxPortEtherOperEgressRate$* kbps
Cause	The tmnxEqPortEtherEgressRateChange notification is generated when the port's operational egress rate changes, due to the reception of ETH-BN (Ethernet Bandwidth Notification) messages, or from a configuration change.
Effect	N/A
Recovery	N/A

58.56 tmnxEqPortEtherInternalAlarm

Table 1199: tmnxEqPortEtherInternalAlarm properties

Property name	Value
Application name	PORT
Event ID	2054
Event name	tmnxEqPortEtherInternalAlarm

Property name	Value
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.54
Default severity	minor
Source stream	main
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 effect.
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'.

58.57 tmnxEqPortEtherInternalAlarmClr

Table 1200: 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
Source stream	main
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.
Effect	N/A
Recovery	N/A

58.58 tmnxEqPortEtherSymMonAlarm

Table 1201: 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
Source stream	main
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.

58.59 tmnxEqPortEtherSymMonAlarmClear

Table 1202: tmnxEqPortEtherSymMonAlarmClear properties

Property name	Value
Application name	PORT
Event ID	2058
Event name	tmnxEqPortEtherSymMonAlarmClear

Property name	Value
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.58
Default severity	minor
Source stream	main
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

58.60 tmnxEqPortFlexEGroupAlrm

Table 1203: tmnxEqPortFlexEGroupAlrm properties

Property name	Value
Application name	PORT
Event ID	2097
Event name	tmnxEqPortFlexEGroupAlrm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.78
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortFlexEGrpAlmReason$* set
Cause	This log event is generated when a FlexE group level port alarm condition is detected. It is generated only when the type of alarm being raised is enabled in tmnxMdaFlexGroupReportAlarm
Effect	N/A
Recovery	N/A

58.61 tmnxEqPortFlexEGroupAlrmClr

Table 1204: tmnxEqPortFlexEGroupAlrmClr properties

Property name	Value
Application name	PORT
Event ID	2098
Event name	tmnxEqPortFlexEGroupAlrmClr
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.79
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortFlexEGrpAlmReason$* clear
Cause	This log event is generated when a FlexE group level port alarm condition is cleared. It is generated only when the type of alarm being raised is enabled in tmnxMdaFlexGroupReportAlarm
Effect	N/A
Recovery	N/A

58.62 tmnxEqPortFlexEMbrPhyInstAlrm

Table 1205: tmnxEqPortFlexEMbrPhyInstAlrm properties

Property name	Value
Application name	PORT
Event ID	2101
Event name	tmnxEqPortFlexEMbrPhyInstAlrm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.82
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortFlexEMbrPhyInstAlmReason$* set

Property name	Value
Cause	This log event is generated when a FlexE port alarm condition is detected on a FlexE 100G PHY Instance. It is generated only when the type of alarm being raised is enabled in tmnxMdaFlexMemberPhy ReportAlarm
Effect	N/A
Recovery	N/A

58.63 tmnxEqPortFlexEMbrPhyInstAlrmClr

Table 1206: tmnxEqPortFlexEMbrPhyInstAlrmClr properties

Property name	Value
Application name	PORT
Event ID	2102
Event name	tmnxEqPortFlexEMbrPhyInstAlrmClr
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.83
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortFlexEMbrPhyInstAlmReason$* clear
Cause	This log event is generated when a FlexE port alarm condition is cleared on a FlexE 100G PHY Instance. It is generated only when the type of alarm being raised is enabled in tmnxMdaFlexMemberPhy ReportAlarm
Effect	N/A
Recovery	N/A

58.64 tmnxEqPortFlexEMemberAlrm

Table 1207: tmnxEqPortFlexEMemberAlrm properties

Property name	Value
Application name	PORT
Event ID	2099
Event name	tmnxEqPortFlexEMemberAlrm
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.80
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortFlexEMbrAlmReason$* set
Cause	This log event is generated when a FlexE port alarm condition is detected on a FlexE member. It is generated only when the type of alarm being raised is enabled in tmnxMdaFlexMemberReportAlarm
Effect	N/A
Recovery	N/A

58.65 tmnxEqPortFlexEMemberAlrmClr

Table 1208: tmnxEqPortFlexEMemberAlrmClr properties

Property name	Value
Application name	PORT
Event ID	2100
Event name	tmnxEqPortFlexEMemberAlrmClr
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.81
Default severity	minor
Source stream	main
Message format string	Alarm *$tmnxPortFlexEMbrAlmReason$* clear
Cause	This log event is generated when a FlexE port alarm condition is cleared on a FlexE member. It is generated only when the type of alarm being raised is enabled in tmnxMdaFlexMemberReportAlarm

Property name	Value
Effect	N/A
Recovery	N/A

58.66 tmnxEqSonetClockSrcNotCompatible

Table 1209: 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
Source stream	main
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.

58.67 tmnxEqSonetFramingNotCompatible

Table 1210: 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
Source stream	main
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 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.

58.68 tmnxEqSonetSfThreshNotCompatible

Table 1211: 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
Source stream	main

Property name	Value
Message format string	Configured SONET/SDH SF threshold 10e-*$tmnxSonetBerSfThreshold $* not compatible with MDA type *$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.

58.69 tmnxHwAggShpSchedOperColorAmber

Table 1212: tmnxHwAggShpSchedOperColorAmber properties

Property name	Value
Application name	PORT
Event ID	2083
Event name	tmnxHwAggShpSchedOperColorAmber
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.68
Default severity	minor
Source stream	main
Message format string	Hw-agg-shaper-scheduler Amber Alarm
Cause	The notification tmnxHwAggShpSchedOperColorAmber is generated when the number of hw-agg-shapers for an object (Vport) hw-agg-shaper-scheduler policy has crossed 90% of scaling threshold.
Effect	Hw Agg shaper scheduler algorithm will stop running.
Recovery	Monitor the hw-agg-shappers closely within the hw-agg-shapper-scheduler policy.

58.70 tmnxHwAggShpSchedOperColorGreen

Table 1213: tmnxHwAggShpSchedOperColorGreen properties

Property name	Value
Application name	PORT
Event ID	2082
Event name	tmnxHwAggShpSchedOperColorGreen
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.67
Default severity	minor
Source stream	main
Message format string	Hw-agg-shaper-scheduler Green Alarm
Cause	The notification tmnxHwAggShpSchedOperColorGreen is generated when the number of hw-agg-shapers for an object (Vport) hw-agg-shaper-scheduler policy is well within thresholds.
Effect	Hw Agg shaper scheduler algorithm is running within the normal parameters.
Recovery	None required.

58.71 tmnxHwAggShpSchedOperColorRed

Table 1214: tmnxHwAggShpSchedOperColorRed properties

Property name	Value
Application name	PORT
Event ID	2084
Event name	tmnxHwAggShpSchedOperColorRed
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.69
Default severity	minor
Source stream	main

Property name	Value
Message format string	Hw-agg-shaper-scheduler Red Alarm
Cause	The notification tmnxHwAggShpSchedOperColorRed is generated when the number of hw-agg-shapers for an object (Vport) hw-agg-shaper-scheduler policy has crossed 100% of scaling threshold.
Effect	Hw Agg shaper scheduler algorithm has stopped running.
Recovery	Reduce the hw-agg-shapers attached to the hw-agg-shapper-scheduler policy.

58.72 tmnxPortAUIReset

Table 1215: tmnxPortAUIReset properties

Property name	Value
Application name	PORT
Event ID	2076
Event name	tmnxPortAUIReset
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.66
Default severity	warning
Source stream	main
Message format string	Reset of the attachment unit interface - likely cause *$tmnxPortNotifyAUIResetSource$*
Cause	This log event is used only for connectorized ports where a CAUI reset is not expected. This may indicate an issue with the optical line feeding into the SFF that is passed through to the system.
Effect	A reset of the AUI will impact all connector-ports on the connector. Generally, AUI resets are recovered immediately but there can be impact to the traffic flow.
Recovery	As this is reporting an unexpected condition related to the external optical line, the line and the SFF should be investigated.

58.73 tmnxPortEtherLoopbackStarted

Table 1216: tmnxPortEtherLoopbackStarted properties

Property name	Value
Application name	PORT
Event ID	2071
Event name	tmnxPortEtherLoopbackStarted
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.63
Default severity	major
Source stream	main
Message format string	Started '*$tmnxPortEtherLoopback$*' loopback on Ethernet port *$tmnx PortPortID$*
Cause	The tmnxPortEtherLoopbackStarted notification is generated when tmnxPortEtherLoopback is modified to set the Ethernet port to a loopback mode.
Effect	Setting the port in loopback mode impacts the normal flow of traffic across the port.
Recovery	Remove loopback on the port to restore normal traffic flow.

58.74 tmnxPortEtherLoopbackStopped

Table 1217: tmnxPortEtherLoopbackStopped properties

Property name	Value
Application name	PORT
Event ID	2072
Event name	tmnxPortEtherLoopbackStopped
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.64
Default severity	major

Property name	Value
Source stream	main
Message format string	Stopped '*$tmnxPortEtherLoopback$*' loopback on Ethernet port *$tmnx PortPortID$*
Cause	The tmnxPortEtherLoopbackStopped notification is generated when a loopback is removed on an Ethernet port. The value of tmnxPortEther Loopback specifies the type of loopback that was configured and has now been removed.
Effect	The loopback has been removed and normal traffic flow may resume.
Recovery	No recovery is required.

58.75 tmnxPortGnssStatusChange

Table 1218: tmnxPortGnssStatusChange properties

Property name	Value
Application name	PORT
Event ID	2073
Event name	tmnxPortGnssStatusChange
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.65
Default severity	major
Source stream	main
Message format string	GNSS port *$tmnxPortPortID$* status changed; sync *$tmnxPortGnss SyncStatus$*, antenna: *$tmnxPortGnssAntennaStatus$*, receiver: *$tmnxPortGnssReceiverStatus$*
Cause	This notification may be triggered for a variety of reasons including (but not limited to): 1) The antenna is experiencing fault issues 2) The number of visible satellites is too low
Effect	The GNSS receiver is not able to provide a sync-worthy clock signal.
Recovery	If the customer is expecting the GNSS receiver to be locked, the customer will need to determine the root cause (for example, insufficient visible satellites) and resolve the issue (for example, ensure tmnxPortGnssElevationMaskAngle is set accordingly)

58.76 tmnxPortUnsupportedFunction

Table 1219: 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	warning
Source stream	main
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.
Effect	N/A
Recovery	N/A

58.77 tmnxResvCbsPoolThreshAmber

Table 1220: 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
Source stream	main

Property name	Value
Message format string	Amber Alarm: CBS over Amber threshold: ObjType=*$tmnxObjType$* Owner= *$tmnxObjPortId$* Type=*$tmnxObjAppType$* Pool=*$tmnxObjAppPool$* ResvSize=*$tmnxObjAppResvSize$* 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 threshold value specified by tmnxObjectAppAmbrAlrmThresh.
Effect	This is warning event but the traffic is not yet affected.
Recovery	The value of tmnxObjectAppResvCbs may need to be adjusted.

58.78 tmnxResvCbsPoolThreshGreen

Table 1221: tmnxResvCbsPoolThreshGreen properties

Property name	Value
Application name	PORT
Event ID	2049
Event name	tmnxResvCbsPoolThreshGreen
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.49
Default severity	minor
Source stream	main
Message format string	Green Alarm: CBS within threshold: ObjType=*$tmnxObjType$* Owner= *$tmnxObjPortId$* Type=*$tmnxObjAppType$* Pool=*$tmnxObjAppPool$* 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.

58.79 tmnxResvCbsPoolThreshRed

Table 1222: 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
Source stream	main
Message format string	Red Alarm: CBS over Red threshold: ObjType=*$tmnxObjType$* Owner= *$tmnxObjPortId$* Type=*$tmnxObjAppType$* Pool=*$tmnxObjAppPool$* ResvSize=*$tmnxObjAppResvSize$* SumOfQ ResvSize= *$tmnxObjAppSumOfQResvSize$* Old ResvCBS=*$tmnxObjAppResvCbsOld$* New ResvCBS=*$tmnxObjAppResvCbsNew$* Old ResvSize= *$tmnxObjAppResvSizeOld$*
Cause	The notification tmnxResvCbsPoolThreshRed is generated when a reserved-CBS of an object (MDA or port) has crossed the threshold value specified by tmnxObjectAppRedAlrmThresh.
Effect	This is a critical event and the traffic may be affected.
Recovery	The value of tmnxObjectAppResvCbs may need to be adjusted.

58.80 tmnxResvPoolUseThreshExcd

Table 1223: tmnxResvPoolUseThreshExcd properties

Property name	Value
Application name	PORT
Event ID	2091
Event name	tmnxResvPoolUseThreshExcd
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.72

Property name	Value
Default severity	minor
Source stream	main
Message format string	Reserved Pool Usage Threshold Exceeded Alarm
Cause	The notification tmnxResvPoolUseThreshExcd is generated when the reserved pool usage has gone above the threshold in the sampling interval. If reserved pool started this new interval below the threshold and if it has gone above threshold at any point during the interval then this trap is generated.
Effect	Reserved pool threshold usage went above the threshold percentage in this sampling interval.
Recovery	User can either increase the threshold percentage or can increase the size of the reserved pool to subside the alarm.

58.81 tmnxResvPoolUseThreshNotExcd

Table 1224: tmnxResvPoolUseThreshNotExcd properties

Property name	Value
Application name	PORT
Event ID	2092
Event name	tmnxResvPoolUseThreshNotExcd
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.73
Default severity	minor
Source stream	main
Message format string	Reserved Pool Usage Threshold Not Exceeded Alarm
Cause	The notification tmnxResvPoolUseThreshNotExcd is generated when the reserved pool usage has gone below the threshold in the sampling interval. If reserved pool started this new interval above the threshold and bounced back to the normal threshold at any point during the interval then this trap is generated.
Effect	Reserved pool threshold usage went below the threshold percentage in this sampling interval.
Recovery	None required.

58.82 tmnxRS232ControlLeadSignalChg

Table 1225: tmnxRS232ControlLeadSignalChg properties

Property name	Value
Application name	PORT
Event ID	2062
Event name	tmnxRS232ControlLeadSignalChg
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.59
Default severity	minor
Source stream	main
Message format string	Serial port *$tmnxPortNotifyPortId$* control leads signal change: *$tmnx PortNotifyLeadsSignalChg$*
Cause	This notification may be triggered for a variety of reasons. One example is that the far-end equipment has been disconnected.
Effect	Alert user of transitions.
Recovery	Determine root cause and resolve accordingly.

58.83 tmnxRS232SquelchResetIssued

Table 1226: tmnxRS232SquelchResetIssued properties

Property name	Value
Application name	PORT
Event ID	2064
Event name	tmnxRS232SquelchResetIssued
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.61
Default severity	minor
Source stream	main

Property name	Value
Message format string	Serial port *$tmnxPortNotifyPortId$* squelch reset issued, existing squelch status: *$tmnxRS232SocketSquelchStatus$*
Cause	N/A
Effect	N/A
Recovery	N/A

58.84 tmnxRS232SquelchStatusChange

Table 1227: tmnxRS232SquelchStatusChange properties

Property name	Value
Application name	PORT
Event ID	2063
Event name	tmnxRS232SquelchStatusChange
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.60
Default severity	minor
Source stream	main
Message format string	Serial port *$tmnxPortNotifyPortId$* squelch status: *$tmnxRS232Socket SquelchStatus$*
Cause	This notification may be triggered for the following reasons: 1) A continuous stream of data is being received for a specified period of time, tmnxRS232SocketSquelchDelay. 2) The continuous stream of data is no longer being received for a specified period of time, tmnxRS232SocketUnsquelchDelay.
Effect	Incoming data will be suppressed or unsuppressed accordingly.
Recovery	Determine root cause of far-end sending continuous data and resolve accordingly.

58.85 tmnxSharedPoolUseThreshExcd

Table 1228: tmnxSharedPoolUseThreshExcd properties

Property name	Value
Application name	PORT
Event ID	2095
Event name	tmnxSharedPoolUseThreshExcd
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.76
Default severity	minor
Source stream	main
Message format string	Shared Pool Usage Threshold Exceeded Alarm
Cause	The notification tmnxSharedPoolUseThreshExcd is generated when the shared pool usage has gone above the threshold in the sampling interval. If shared pool started this new interval below the threshold and if it has gone above threshold at any point during the interval then this trap is generated.
Effect	Shared pool threshold usage went above the threshold percentage in this sampling interval.
Recovery	User can either increase the threshold percentage or can increase the size of the shared pool to subside the alarm.

58.86 tmnxSharedPoolUseThreshNotExcd

Table 1229: tmnxSharedPoolUseThreshNotExcd properties

Property name	Value
Application name	PORT
Event ID	2096
Event name	tmnxSharedPoolUseThreshNotExcd
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.77
Default severity	minor
Source stream	main
Message format string	Shared Pool Usage Threshold Not Exceeded Alarm

Property name	Value
Cause	The notification tmnxSharedPoolUseThreshNotExcd is generated when the shared pool usage has gone below the threshold in the sampling interval. If shared pool started this new interval above the threshold and bounced back to the normal threshold at any point during the interval then this trap is generated.
Effect	Shared pool threshold usage went below the threshold percentage in this sampling interval.
Recovery	None required.

58.87 tmnxTotalPoolUseThreshExcd

Table 1230: tmnxTotalPoolUseThreshExcd properties

Property name	Value
Application name	PORT
Event ID	2093
Event name	tmnxTotalPoolUseThreshExcd
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.74
Default severity	minor
Source stream	main
Message format string	Total Pool Usage Threshold Exceeded Alarm
Cause	The notification tmnxTotalPoolUseThreshExcd is generated when the total pool usage has gone above the threshold in the sampling interval. If total pool started this new interval below the threshold and if it has gone above threshold at any point during the interval then this trap is generated.
Effect	Total pool threshold usage went above the threshold percentage in this sampling interval.
Recovery	User can either increase the threshold percentage or can increase the size of the total pool to subside the alarm.

58.88 tmnxTotalPoolUseThreshNotExcd

Table 1231: tmnxTotalPoolUseThreshNotExcd properties

Property name	Value
Application name	PORT
Event ID	2094
Event name	tmnxTotalPoolUseThreshNotExcd
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.75
Default severity	minor
Source stream	main
Message format string	Total Pool Usage Threshold Not Exceeded Alarm
Cause	The notification tmnxTotalPoolUseThreshNotExcd is generated when the total pool usage has gone below the threshold in the sampling interval. If total pool started this new interval above the threshold and bounced back to the normal threshold at any point during the interval then this trap is generated.
Effect	Total pool threshold usage went below the threshold percentage in this sampling interval.
Recovery	None required.

58.89 tmnxWlanNetworkConnected

Table 1232: tmnxWlanNetworkConnected properties

Property name	Value
Application name	PORT
Event ID	2074
Event name	tmnxWlanNetworkConnected
SNMP notification prefix and OID	TIMETRA-WLAN-MIB.tmnxWlanNotifications.1
Default severity	minor

Property name	Value
Source stream	main
Message format string	Connected to WLAN network *$tmnxWlanNotifyWlanNetworkId$* SSID ' *$tmnxWlanNetworkSSID$*'
Cause	The system generates a tmnxWlanNetworkConnected notification when the system establishes a WLAN connection to the specified network.
Effect	N/A
Recovery	N/A

58.90 tmnxWlanNetworkDisconnected

Table 1233: tmnxWlanNetworkDisconnected properties

Property name	Value
Application name	PORT
Event ID	2075
Event name	tmnxWlanNetworkDisconnected
SNMP notification prefix and OID	TIMETRA-WLAN-MIB.tmnxWlanNotifications.2
Default severity	minor
Source stream	main
Message format string	Disconnected from WLAN network *$tmnxWlanNotifyWlanNetworkId$* SSID ' *$tmnxWlanNetworkSSID$*'
Cause	The system generates a tmnxWlanNetworkDisconnected notification when the system loses the WLAN connection to the specified network.
Effect	N/A
Recovery	N/A

58.91 tPortAccEgrQGrpHostMatchFailure

Table 1234: 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	major
Source stream	main
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

58.92 tPortEgrVPortHostMatchFailure

Table 1235: tPortEgrVPortHostMatchFailure properties

Property name	Value
Application name	PORT
Event ID	2040
Event name	tPortEgrVPortHostMatchFailure
SNMP notification prefix and OID	TIMETRA-PORT-MIB.tmnxPortNotification.42
Default severity	major
Source stream	main
Message format string	Could not find a specific port egress virtual port for host with inter-dest-id ' *$tmnxHostMatchNotifyIntDestId$*', org-string '*$tmnxHostMatchNotify*

Property name	Value
	OrgString$*' and sub-id '*$tmnxHostMatchNotifySubIdent$*' on port *$tmnx PortNotifyPortId$
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

59 PPPOE

59.1 tmnxMlpppBundleIndicatorsChange

Table 1236: 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
Source stream	main
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

59.2 tmnxPppoeLacSteeringActive

Table 1237: tmnxPppoeLacSteeringActive properties

Property name	Value
Application name	PPPOE

Property name	Value
Event ID	2004
Event name	tmnxPppoeLacSteeringActive
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.4
Default severity	warning
Source stream	main
Message format string	The PPPoE/LAC session *$tmnxPppoeLacSteeringSession$* on SAP *$sapEncapValue$* in service *$svcId$* is steered using profile *$tmnx PppoeLacSteeringProfile$*.
Cause	The tmnxPppoeLacSteeringActive notification indicates that the appropriate PPPoE/LAC session is steered.
Effect	N/A
Recovery	N/A

59.3 tmnxPppoeLacSteeringFailed

Table 1238: tmnxPppoeLacSteeringFailed properties

Property name	Value
Application name	PPPOE
Event ID	2006
Event name	tmnxPppoeLacSteeringFailed
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.6
Default severity	warning
Source stream	main
Message format string	The PPPoE/LAC session *$tmnxPppoeLacSteeringSession$* on SAP *$sapEncapValue$* in service *$svcId$* changed to steering failed using profile *$tmnxPppoeLacSteeringProfile$* (*$tmnxPppoeLacSteering Failure$*).
Cause	The tmnxPppoeLacSteeringFailed notification indicates that steering has failed. The problem is described in the object tmnxPppoeLac SteeringFailure.

Property name	Value
Effect	N/A
Recovery	N/A

59.4 tmnxPppoeLacSteeringStopped

Table 1239: tmnxPppoeLacSteeringStopped properties

Property name	Value
Application name	PPPOE
Event ID	2005
Event name	tmnxPppoeLacSteeringStopped
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.5
Default severity	warning
Source stream	main
Message format string	The PPPoE/LAC session *$tmnxPppoeLacSteeringSession$* on SAP *$sapEncapValue$* in service *$svcId$* has stopped steering using profile *$tmnxPppoeLacSteeringProfile$*.
Cause	The tmnxPppoeLacSteeringStopped notification indicates that the appropriate steered PPPoE/LAC session has stopped steering. To make the session steered again, a COA with the appropriate steering profile has to be sent
Effect	N/A
Recovery	N/A

59.5 tmnxPppoeMaxSessionsOvrExceeded

Table 1240: tmnxPppoeMaxSessionsOvrExceeded properties

Property name	Value
Application name	PPPOE

Property name	Value
Event ID	2007
Event name	tmnxPppoeMaxSessionsOvrExceeded
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.7
Default severity	warning
Source stream	main
Message format string	PPPoE max sessions override exceeded on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxPppoeMaxSessionsOvrReason$*
Cause	The tmnxPppoeMaxSessionsOvrExceeded notification indicates the configured maximum number of sessions has been reached. Detailed information is provided in the object tmnxPppoeMaxSessionsOvr Reason.
Effect	N/A
Recovery	No recovery is necessary.

59.6 tmnxPppoeNcpFailure

Table 1241: tmnxPppoeNcpFailure properties

Property name	Value
Application name	PPPOE
Event ID	2002
Event name	tmnxPppoeNcpFailure
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.2
Default severity	warning
Source stream	main
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

Property name	Value
Recovery	N/A

59.7 tmnxPppoeSessionFailure

Table 1242: 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
Source stream	main
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.

60 PPPOE_CLNT

60.1 tmnxPppoeClientEchoTimeout

Table 1243: tmnxPppoeClientEchoTimeout properties

Property name	Value
Application name	PPPOE_CLNT
Event ID	2004
Event name	tmnxPppoeClientEchoTimeout
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeClntNotifications.2
Default severity	minor
Source stream	main
Message format string	PPPoE client *$tmnxPppoeClntIdent$* encountered an LCP echo timeout
Cause	The tmnxPppoeClientEchoTimeout notification indicates that the specified PPPoE client encountered an LCP echo timeout.
Effect	N/A
Recovery	N/A

60.2 tmnxPppoeClientNcpFailure

Table 1244: tmnxPppoeClientNcpFailure properties

Property name	Value
Application name	PPPOE_CLNT
Event ID	2005
Event name	tmnxPppoeClientNcpFailure

Property name	Value
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeClntNotifications.3
Default severity	minor
Source stream	main
Message format string	PPPoE client NCP phase setup failure for *$tmnxPppoeClntIdent$* - protocol *$tmnxPppoeNcpFailureProtocol$*
Cause	The tmnxPppoeClientNcpFailure notification indicates that the specified PPPoE client encountered a NCP phase setup failure.
Effect	N/A
Recovery	N/A

60.3 tmnxPppoeClientSetupFailure

Table 1245: tmnxPppoeClientSetupFailure properties

Property name	Value
Application name	PPPOE_CLNT
Event ID	2001
Event name	tmnxPppoeClientSetupFailure
SNMP notification prefix and OID	TIMETRA-PPPOE-MIB.tmnxPppoeClntNotifications.1
Default severity	minor
Source stream	main
Message format string	PPPoE client setup failure for *$tmnxPppoeClntIdent$*
Cause	The tmnxPppoeClientSetupFailure notification indicates that the specified PPPoE client encountered a failure during setup.
Effect	N/A
Recovery	N/A

61 PTP

61.1 tmnxPtpCardNotSupported

Table 1246: 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
Source stream	main
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.

61.2 tmnxPtpCardNotSupportedClear

Table 1247: tmnxPtpCardNotSupportedClear properties

Property name	Value
Application name	PTP
Event ID	2002
Event name	tmnxPtpCardNotSupportedClear
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.2
Default severity	minor
Source stream	main
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

61.3 tmnxPtpClockRecoveryStateChange

Table 1248: 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
Source stream	main
Message format string	IEEE1588 (PTP) Frequency Recovery state: *$tmnxPtpClockRecovery State$*

Property name	Value
Cause	The tmnxPtpClockRecoveryStateChange is generated when the Precision Timing Protocol (PTP) clock recovery state changes on the system.
Effect	N/A
Recovery	N/A

61.4 tmnxPtpDynamicChange

Table 1249: 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
Source stream	main
Message format string	IEEE1588 (PTP) *$tmnxPtpNotifyRowDescription$*
Cause	The tmnxPtpDynamicChange notification is generated when an object dynamically (i.e. not by configuration) changes state. This notification identifies the affected row.
Effect	N/A
Recovery	N/A

61.5 tmnxPtpMasterClockChangedEvent

Table 1250: tmnxPtpMasterClockChangedEvent properties

Property name	Value
Application name	PTP

Property name	Value
Event ID	2003
Event name	tmnxPtpMasterClockChangedEvent
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.3
Default severity	minor
Source stream	main
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

61.6 tmnxPtpOutOfResources

Table 1251: 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
Source stream	main
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

Property name	Value
	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. tmnxPtpOutOfResourcesClear is generated when this event is cleared.
Effect	N/A
Recovery	N/A

61.7 tmnxPtpOutOfResourcesClear

Table 1252: 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
Source stream	main
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

61.8 tmnxPtpPeerNoRxTimestamping

Table 1253: tmnxPtpPeerNoRxTimestamping properties

Property name	Value
Application name	PTP
Event ID	2015
Event name	tmnxPtpPeerNoRxTimestamping
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.15
Default severity	minor
Source stream	main
Message format string	Timestamping of receive communications with peer *$tmnxPtpPeer IpAddress$* is performed at the CPM. Performance may be degraded.
Cause	The tmnxPtpPeerNoRxTimestamping notification is generated on initial exchange of PTP event messages with a peer and whenever the location of the timestamping of the event messages received from the peer changes, and the location is 'cpm (2)'.
Effect	When the timestamping location is 'cpm (2)', the accuracy of the PTP event messages is less then if the messages are timestamped at the port and performance will be negatively impacted.
Recovery	It may be necessary to check the capabilities of the port being used for the messages and/or to modify routing to direct the messages to an alternate port. Some reasons for a port to not perform timestamping include: not configured, port not configured for ptp-hw-assist, port does not support ptp-hw-assist.

61.9 tmnxPtpPeerNoRxTimestampingClear

Table 1254: tmnxPtpPeerNoRxTimestampingClear properties

Property name	Value
Application name	PTP
Event ID	2016
Event name	tmnxPtpPeerNoRxTimestampingClear
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.16
Default severity	minor

Property name	Value
Source stream	main
Message format string	Timestamping of receive communications with peer *$tmnxPtpPeer IpAddress$* is now performed at the port.
Cause	The tmnxPtpPeerNoRxTimestampingClear notification is generated when the conditions that caused the tmnxPtpPeerNoRxTimestamping event have been resolved and result in the location of the timestamping of the event messages received from the peer being changed from 'cpm (2)' to 'port (1)'.
Effect	When the timestamping location is the 'port (2)', the accuracy of the PTP event messages is optimal.
Recovery	No recovery is required for this notification.

61.10 tmnxPtpPeerNoTxTimestamping

Table 1255: tmnxPtpPeerNoTxTimestamping properties

Property name	Value
Application name	PTP
Event ID	2013
Event name	tmnxPtpPeerNoTxTimestamping
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.13
Default severity	minor
Source stream	main
Message format string	Timestamping of transmit communications with peer *$tmnxPtpPeer IpAddress$* is performed at the CPM. Performance may be degraded.
Cause	The tmnxPtpPeerNoTxTimestamping notification is generated on initial exchange of PTP event messages with a peer and whenever the location of the timestamping of the event messages transmitted to the peer changes, and the location is 'cpm (2)'.
Effect	When the timestamping location is 'cpm (2)', the accuracy of the PTP event messages is less then if the messages are timestamped at the port and performance will be negatively impacted.
Recovery	It may be necessary to check the capabilities of the port being used for the messages and/or to modify routing to direct the messages to an

Property name	Value
	alternate port. Some reasons for a port to not perform timestamping include: not configured, port not configured for ptp-hw-assist, port does not support ptp-hw-assist.

61.11 tmnxPtpPeerNoTxTimestampingClear

Table 1256: tmnxPtpPeerNoTxTimestampingClear properties

Property name	Value
Application name	PTP
Event ID	2014
Event name	tmnxPtpPeerNoTxTimestampingClear
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.14
Default severity	minor
Source stream	main
Message format string	Timestamping of transmit communications with peer *$tmnxPtpPeer IpAddress$* is now performed at the port.
Cause	The tmnxPtpPeerNoTxTimestampingClear notification is generated when the conditions that caused the tmnxPtpPeerNoTxTimestamping event have been resolved and result in the location of the timestamping of the event messages transmitted to the peer being changed from 'cpm (2)' to 'port (1)'.
Effect	When the timestamping location is the 'port (2)', the accuracy of the PTP event messages is optimal.
Recovery	No recovery is required for this notification.

61.12 tmnxPtpPortNoTimestamping

Table 1257: tmnxPtpPortNoTimestamping properties

Property name	Value
Application name	PTP

Property name	Value
Event ID	2008
Event name	tmnxPtpPortNoTimestamping
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.8
Default severity	minor
Source stream	main
Message format string	Port *$tmnxPtpNotifyPortId$* does not support PTP port-based timestamping. 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.

61.13 tmnxPtpPortPtsfUnusable

Table 1258: tmnxPtpPortPtsfUnusable properties

Property name	Value
Application name	PTP
Event ID	2009
Event name	tmnxPtpPortPtsfUnusable
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.9
Default severity	minor
Source stream	main
Message format string	Packet timing signal from PTP port *$tmnxPortPortID$* neighbor *$tmnxPtpPortNeighborMacAddress$* is unusable.
Cause	The PTP process detected excessive noise between the local port and the indicated external Master port.

Property name	Value
Effect	Any Announce messages received from the indicated neighbor shall be excluded from the BMCA algorithm until this condition is cleared.
Recovery	The cause of the excessive noise should be identified and corrected. Once resolved, the clear command for this neighbor port must be executed to clear the condition and allow Announces from this neighbor to be considered in the BMCA.

61.14 tmnxPtpRequiresSystemReboot

Table 1259: tmnxPtpRequiresSystemReboot properties

Property name	Value
Application name	PTP
Event ID	2010
Event name	tmnxPtpRequiresSystemReboot
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.10
Default severity	major
Source stream	main
Message format string	The PTP configuration (clock-type *$tmnxPtpClockClockType$*, profile *$tmnxPtpClockProfile$*) is different than the initial configuration (clock-type *$tmnxPtpNotifyInitialClockType$*, profile *$tmnxPtpNotifyInitial Profile$*). A system reboot is required for the change to take effect.
Cause	The PTP configuration has changed since system initialization. On some SROS series systems, changing the tmnxPtpClockClockType or tmnxPtpClockProfile requires a system reboot to take effect.
Effect	PTP remains operationally out of service, even though it has been administratively enabled.
Recovery	Reboot the system, or change the clock configuration to the original configuration.

61.15 tmnxPtpRequiresSystemRebootClear

Table 1260: tmnxPtpRequiresSystemRebootClear properties

Property name	Value
Application name	PTP
Event ID	2011
Event name	tmnxPtpRequiresSystemRebootClear
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.11
Default severity	cleared
Source stream	main
Message format string	The PTP configuration has changed to the initial configuration. A system reboot is no longer required.
Cause	The system generates the tmnxPtpRequiresSystemRebootClear notification when the user changes the PTP configuration to match the initial configuration.
Effect	PTP does not require a system reboot to become operationally in service.
Recovery	There is no recovery required for this notification.

61.16 tmnxPtpTimeRecoveryStateChange

Table 1261: tmnxPtpTimeRecoveryStateChange properties

Property name	Value
Application name	PTP
Event ID	2012
Event name	tmnxPtpTimeRecoveryStateChange
SNMP notification prefix and OID	TIMETRA-PTP-MIB.tmnxPtp1588Notifications.12
Default severity	minor
Source stream	main
Message format string	IEEE1588 (PTP) Time Recovery state: *$tmnxPtpTimeRecoveryState$*

Property name	Value
Cause	The tmnxPtpTimeRecoveryStateChange is generated when the Precision Timing Protocol (PTP) time recovery state changes on the system.
Effect	N/A
Recovery	N/A

62 PYTHON

62.1 tmnxPythonInterpreterRestarted

Table 1262: tmnxPythonInterpreterRestarted properties

Property name	Value
Application name	PYTHON
Event ID	2001
Event name	tmnxPythonInterpreterRestarted
SNMP notification prefix and OID	TIMETRA-PYTHON-MIB.tmnxPythonNotifications.1
Default severity	warning
Source stream	main
Message format string	The Python interpreter ' *$tmnxPythonNotifyInterpreter$*' has restarted - *$tmnxPythonNotifyString$*
Cause	The tmnxPythonInterpreterRestarted notification is sent when a Python interpreter instance restarted. The reason is typically a lack of memory. The object tmnxPythonNotifyInterpreter indicates name of the interpreter, and the object tmnxPythonNotifyString indicates the reason of the restart.
Effect	The effect depends on the application that was executing the Python script.
Recovery	If this event occurs repeatedly, the exact cause should be determined. The exact cause will reveal what recovery actions are appropriate.

63 RADIUS

63.1 tmnxRadAcctOnOngoing

Table 1263: 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
Source stream	main
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 indefinitely.

63.2 tmnxRadRouteDownloadFailed

Table 1264: tmnxRadRouteDownloadFailed properties

Property name	Value
Application name	RADIUS
Event ID	2002
Event name	tmnxRadRouteDownloadFailed

Property name	Value
SNMP notification prefix and OID	TIMETRA-RADIUS-MIB.tmnxRadProxNotifications.2
Default severity	minor
Source stream	main
Message format string	RADIUS route download failed : *$tmnxRadiusAdditionalInfo$*
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.

63.3 tmnxRadSrvPlcySrvOperStateCh

Table 1265: 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
Source stream	main
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

Property name	Value
	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 of the RADIUS server(s) may have to be increased, or the values of the objects mentioned above may have to be adapted.

64 RIP

64.1 ripPacketDiscarded

Table 1266: ripPacketDiscarded properties

Property name	Value
Application name	RIP
Event ID	2001
Event name	ripPacketDiscarded
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	Discarded packet from *$ripPacketSrcIp$* received on interface *$vRtr IfIndex$* 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

64.2 vRtrRipAuthTypeFailure

Table 1267: vRtrRipAuthTypeFailure properties

Property name	Value
Application name	RIP
Event ID	2003

Property name	Value
Event name	vRtrRipAuthTypeFailure
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.2
Default severity	minor
Source stream	main
Message format string	Authentication type failure on packet received from peer *$vRtrRipPeer Address$* on interface *$vRtrRipPeerIfIndex$*
Cause	The authentication key in a received RIPv2 packet conflicted with the authentication key configured for this router.
Effect	N/A
Recovery	N/A

64.3 vRtrRipAuthTypeMismatch

Table 1268: 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
Source stream	main
Message format string	Authentication type mismatch on packet received from peer *$vRtrRip PeerAddress$* on interface *$vRtrRipPeerIfIndex$*
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

64.4 vRtrRipInstanceExpLmtReached

Table 1269: vRtrRipInstanceExpLmtReached properties

Property name	Value
Application name	RIP
Event ID	2006
Event name	vRtrRipInstanceExpLmtReached
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.5
Default severity	major
Source stream	main
Message format string	RIP instance has reached the export limit *$vRtrRipInstanceExportLimit $*, 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.

64.5 vRtrRipInstanceExpLmtWarning

Table 1270: 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
Source stream	main

Property name	Value
Message format string	RIP instance has reached *$vRtrRipInstanceExpLmtLogPercent$* 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

64.6 vRtrRipInstanceRestarted

Table 1271: 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
Source stream	main
Message format string	RIP instance 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

64.7 vRtrRipInstanceRtsExpLmtDropped

Table 1272: 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
Source stream	main
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

64.8 vRtrRipInstanceShuttingDown

Table 1273: 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
Source stream	main
Message format string	RIP instance is being operationally 'shutdown' because *$ripInstance ShuttingDownReason$*
Cause	The RIP instance shut down on its own accord when the protocol ran out of resources such as memory.

Property name	Value
Effect	N/A
Recovery	The instance will attempt to restart within 30 seconds of shutting down.

64.9 vRtrRipPeerBfdDown

Table 1274: vRtrRipPeerBfdDown properties

Property name	Value
Application name	RIP
Event ID	2010
Event name	vRtrRipPeerBfdDown
SNMP notification prefix and OID	TIMETRA-RIP-MIB.vRtrRipNotifications.8
Default severity	warning
Source stream	main
Message format string	RIP peer *$vRtrRipPeerAddress$* on interface *$vRtrRipPeerIfIndex$* went down due to a BFD session failure
Cause	A RIP peer is presumed down because of a BFD session failure.
Effect	All routes learned from the peer will be removed from the routing table.
Recovery	N/A

65 RIP_NG

65.1 tmnxRipNgAuthFailure

Table 1275: 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
Source stream	main
Message format string	Authentication type failure on *$tmnxRipNgInstVersion$* packet received from peer *$tmnxRipNgPeerAddress$* on interface *$tmnxRipNgPeer IfIndex$*
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

65.2 tmnxRipNgAuthTypeMismatch

Table 1276: tmnxRipNgAuthTypeMismatch properties

Property name	Value
Application name	RIP_NG
Event ID	2002

Property name	Value
Event name	tmnxRipNgAuthTypeMismatch
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.1
Default severity	minor
Source stream	main
Message format string	Authentication type mismatch on *$tmnxRipNgInstVersion$* packet received from peer *$tmnxRipNgPeerAddress$* on interface *$tmnxRip NgPeerIfIndex$*
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

65.3 tmnxRipNgIfUcastAddrNotUsed

Table 1277: 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
Source stream	main
Message format string	*$tmnxRipNgInstVersion$* neighbor *$vRtrIfIndex$* has unicast addresses configured while send mode is not set to 'unicast'
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

65.4 tmnxRipNgInstExpLmtReached

Table 1278: 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
Default severity	minor
Source stream	main
Message format string	*$tmnxRipNgInstVersion$* instance has reached the export limit *$tmnx RipNgInstExportLimit$*, additional routes will not be exported into the instance
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

65.5 tmnxRipNgInstExpLmtWarning

Table 1279: 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

Property name	Value
Source stream	main
Message format string	*$tmnxRipNgInstVersion$* instance has reached *$tmnxRipNgInstExpLmtLogPct$* percent of the export limit *$tmnxRipNgInstExportLimit$*
Cause	A tmnxRipNgInstExpLmtWarning notification is generated when the number of exported routes is equal to the configured percent, tmnxRipNgInstExpLmtLogPct 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

65.6 tmnxRipNgInstRestarted

Table 1280: 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
Source stream	main
Message format string	*$tmnxRipNgInstVersion$* instance restarted
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

65.7 tmnxRipNgInstRtsExpLmtDropped

Table 1281: 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
Source stream	main
Message format string	The number of redistributed routes into the *$tmnxRipNgInstVersion$* instance has dropped below the export limit *$tmnxRipNgInstExportLimit$*
Cause	A tmnxRipNgInstRtsExpLmtDropped notification is generated when the number of exported routes drops below the export limit, tmnxRipNgInstExportLimit.
Effect	N/A
Recovery	N/A

65.8 tmnxRipNgInstShuttingDown

Table 1282: 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

Property name	Value
Source stream	main
Message format string	*$tmnxRipNgInstVersion$* instance is being operationally 'shutdown' because *$tmnxRipNgNotifyReason$*
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

65.9 tmnxRipNgPacketDiscarded

Table 1283: tmnxRipNgPacketDiscarded properties

Property name	Value
Application name	RIP_NG
Event ID	2001
Event name	tmnxRipNgPacketDiscarded
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	Discarded *$tmnxRipNgInstVersion$* packet received from *$tmnx RipNgNotifySrcAddr$* on interface *$vRtrIfIndex$* because *$tmnxRip NgNotifyReason$*
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 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

65.10 tmnxRipNgPeerBfdDown

Table 1284: tmnxRipNgPeerBfdDown properties

Property name	Value
Application name	RIP_NG
Event ID	2010
Event name	tmnxRipNgPeerBfdDown
SNMP notification prefix and OID	TIMETRA-RIP-NG-MIB.tmnxRipNgNotifications.9
Default severity	warning
Source stream	main
Message format string	*$tmnxRipNgInstVersion$* peer *$tmnxRipNgPeerAddress$* on interface *$tmnxRipNgPeerIfIndex$* went down due to a BFD session failure
Cause	A peer is presumed down because of a BFD session failure.
Effect	All routes learned from the peer will be removed from the routing table.
Recovery	N/A

66 ROUTE_POLICY

66.1 trigPolicyPrevEval

Table 1285: 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
Source stream	main
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.

67 RPKI

67.1 tmnxRpkiNotifySession

Table 1286: 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
Source stream	main
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.

67.2 tmnxRpkiStaleTimerExpiry

Table 1287: tmnxRpkiStaleTimerExpiry properties

Property name	Value
Application name	RPKI
Event ID	2002
Event name	tmnxRpkiStaleTimerExpiry
SNMP notification prefix and OID	TIMETRA-RPKI-MIB.tmnxRpkiNotifications.2
Default severity	minor
Source stream	main
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 back up 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. 4) The RPKI server sends a Cache Reset in response to a Serial Query instead of doing an incremental update.
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.

68 RSVP

68.1 vRtrRsvpIfNbrStateDown

Table 1288: 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
Source stream	main
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

68.2 vRtrRsvpIfNbrStateUp

Table 1289: vRtrRsvpIfNbrStateUp properties

Property name	Value
Application name	RSVP
Event ID	2003
Event name	vRtrRsvpIfNbrStateUp
SNMP notification prefix and OID	TIMETRA-RSVP-MIB.tmnxRsvpNotifications.3

Property name	Value
Default severity	warning
Source stream	main
Message format string	Neighbor *$vRtrRsvpNbrAddress$* on interface *$ifIndex$* changed to active state
Cause	A RSVP interface neighbor changed to the active state.
Effect	N/A
Recovery	N/A

68.3 vRtrRsvpIfStateChange

Table 1290: 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
Source stream	main
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.

68.4 vRtrRsvpPEFailOverPriToStdBy

Table 1291: 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
Source stream	main
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.

68.5 vRtrRsvpPEFailOverStdByToPri

Table 1292: 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
Source stream	main

Property name	Value
Message format string	Traffic switched for MVPN instance *$vRtrID$* from standby PE *$vRtrPimNgMvpnUMHPEStandbyAddr$* to primary PE *$vRtrPimNgMvpnUMHPEAddr$*
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 vRtrPimNgMvpnUMHPEAddrType and vRtrPimNgMvpnUMHPEAddr indexes of the varbinds in this notification.
Effect	The tunnel traffic may be affected.
Recovery	None required.

68.6 vRtrRsvpStateChange

Table 1293: 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
Source stream	main
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.

69 SATELLITE

69.1 tmnxSatelliteOperStateChange

Table 1294: 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
Source stream	main
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.

69.2 tmnxSatLocalForwardSapStateChg

Table 1295: tmnxSatLocalForwardSapStateChg properties

Property name	Value
Application name	SATELLITE
Event ID	2017
Event name	tmnxSatLocalForwardSapStateChg
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.17
Default severity	minor
Source stream	main
Message format string	Satellite Local Forward *$tmnxSatLocalForwardId$* SAP *$tmnxSatPortId$*: *$tmnxSatEncapValue$* changed to administrative state: *$tmnxSatLocalForwardSapAdminState$*, operational state: *$tmnxSatLocalForwardSapOperState$*
Cause	The tmnxSatLocalForwardSapStateChg notification is generated when the system detects a change in the administrative state, or operational state of the satellite local forward SAP.
Effect	The administrative state or operational state of the satellite local forward SAP has changed.
Recovery	If the administrative state is 'inService (2)', and the operational state is 'down (2)', check to ensure valid configuration of the satellite local forward SAP, and verify the connection of the satellite to the host. Contact Nokia customer support if the issue cannot be resolved.

69.3 tmnxSatLocalForwardStateChg

Table 1296: tmnxSatLocalForwardStateChg properties

Property name	Value
Application name	SATELLITE
Event ID	2016
Event name	tmnxSatLocalForwardStateChg
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.16
Default severity	minor

Property name	Value
Source stream	main
Message format string	Satellite Local Forward *$tmnxSatLocalForwardId$* changed to administrative state: *$tmnxSatLocalForwardAdminState$*, operational state: *$tmnxSatLocalForwardOperState$*
Cause	The tmnxSatLocalForwardStateChg notification is generated when the system detects a change in the administrative state, or operational state of the satellite local forward.
Effect	The administrative state or operational state of the satellite local forward has changed.
Recovery	If the administrative state is 'inService (2)', and the operational state is 'down (2)', check to ensure valid configuration of the satellite local forward, and verify the connection of the satellite to the host. Contact Nokia\ customer support if the issue cannot be resolved.

69.4 tmnxSatSyncIfTimHoldover

Table 1297: tmnxSatSyncIfTimHoldover properties

Property name	Value
Application name	SATELLITE
Event ID	2006
Event name	tmnxSatSyncIfTimHoldover
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.6
Default severity	critical
Source stream	main
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.

Property name	Value
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.

69.5 tmnxSatSyncIfTimHoldoverClear

Table 1298: 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
Source stream	main
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.

69.6 tmnxSatSyncIfTimRef1Alarm

Table 1299: tmnxSatSyncIfTimRef1Alarm properties

Property name	Value
Application name	SATELLITE
Event ID	2008

Property name	Value
Event name	tmnxSatSyncIfTimRef1Alarm
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.8
Default severity	minor
Source stream	main
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.

69.7 tmnxSatSyncIfTimRef1AlarmClear

Table 1300: 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
Source stream	main
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.
Recovery	No recovery required.

69.8 tmnxSatSyncIfTimRef1Quality

Table 1301: 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
Source stream	main
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.

69.9 tmnxSatSyncIfTimRef2Alarm

Table 1302: 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
Source stream	main

Property name	Value
Message format string	Synchronous timing interface on satellite *$tmnxHwIndex$*, alarm *$tmnxSatNotifySyncIfTimRefAlarm$* on reference 2
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.

69.10 tmnxSatSyncIfTimRef2AlarmClear

Table 1303: 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
Source stream	main
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.

69.11 tmnxSatSyncIfTimRef2Quality

Table 1304: tmnxSatSyncIfTimRef2Quality properties

Property name	Value
Application name	SATELLITE
Event ID	2005
Event name	tmnxSatSyncIfTimRef2Quality
SNMP notification prefix and OID	TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.5
Default severity	minor
Source stream	main
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.

69.12 tmnxSatSyncIfTimRefSwitch

Table 1305: 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
Source stream	main
Message format string	Synchronous timing interface on satellite *$tmnxSatId$*, timing reference changed to *$tmnxSatSyncIfTimingRef1InUse$*

Property name	Value
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.

69.13 tmnxSatSyncIfTimSystemQuality

Table 1306: 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
Source stream	main
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.

70 SECURITY

70.1 cli_user_login

Table 1307: 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
Source stream	security
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

70.2 cli_user_login_failed

Table 1308: 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

Property name	Value
Default severity	minor
Source stream	security
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

70.3 cli_user_login_max_attempts

Table 1309: 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
Source stream	security
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 session 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

Property name	Value
	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.

70.4 cli_user_logout

Table 1310: 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
Source stream	security
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

70.5 enable_admin

Table 1311: enable_admin properties

Property name	Value
Application name	SECURITY
Event ID	2022

Property name	Value
Event name	enable_admin
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	security
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

70.6 ftp_transfer_failed

Table 1312: 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
Source stream	security
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

70.7 ftp_transfer_successful

Table 1313: 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
Source stream	security
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

70.8 ftp_user_login

Table 1314: 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
Source stream	security
Message format string	User *$userName$* from *$srcAddr$* logged in

Property name	Value
Cause	A user was successfully authenticated for login.
Effect	A user access session was started
Recovery	No recovery is required

70.9 ftp_user_login_failed

Table 1315: 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
Source stream	security
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

70.10 ftp_user_login_max_attempts

Table 1316: ftp_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2008

Property name	Value
Event name	ftp_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.47
Default severity	minor
Source stream	security
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 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 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 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.

70.11 ftp_user_logout

Table 1317: 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

Property name	Value
Source stream	security
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.

70.12 grpc_auth

Table 1318: grpc_auth properties

Property name	Value
Application name	SECURITY
Event ID	2229
Event name	grpc_auth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC authorized
Cause	The user called an authorized RPC in the gRPC interface.
Effect	The RPC was processed.
Recovery	No recovery is required.

70.13 grpc_unauth

Table 1319: grpc_unauth properties

Property name	Value
Application name	SECURITY
Event ID	2230
Event name	grpc_unauth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC unauthorized
Cause	The user called an unauthorized RPC in the gRPC interface.
Effect	The RPC was not processed.
Recovery	No recovery is required.

70.14 grpc_user_login

Table 1320: grpc_user_login properties

Property name	Value
Application name	SECURITY
Event ID	2117
Event name	grpc_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
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

70.15 grpc_user_login_failed

Table 1321: grpc_user_login_failed properties

Property name	Value
Application name	SECURITY
Event ID	2119
Event name	grpc_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
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

70.16 grpc_user_login_max_attempts

Table 1322: grpc_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2120
Event name	grpc_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in, user is locked out

Property name	Value
Cause	A user failed to authenticate in more than the permitted number of retries.
Effect	The gRPC session was terminated.
Recovery	No recovery is required.

70.17 grpc_user_logout

Table 1323: grpc_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2118
Event name	grpc_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
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.

70.18 host_snmp_attempts

Table 1324: host_snmp_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2023

Property name	Value
Event name	host_snmp_attempts
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	security
Message format string	Host *$hostAddress$* is locked out for *$lockoutTime$* minutes since it exceeded the configured threshold of unsuccessful SNMP connection attempts.
Cause	The remote SNMP host exceeded 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

70.19 mafEntryMatch

Table 1325: mafEntryMatch properties

Property name	Value
Application name	SECURITY
Event ID	2019
Event name	mafEntryMatch
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	security
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

Property name	Value
Recovery	No recovery is necessary.

70.20 md_cli_io

Table 1326: md_cli_io properties

Property name	Value
Application name	SECURITY
Event ID	2223
Event name	md_cli_io
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	Possible messages: • User *$userName$* from *$srcAddr$* [session ID *$sessionId$*]: *$command$* • User *$userName$* from *$srcAddr$* [session ID *$sessionId$*]: *$prompt$ $command$*
Cause	The user entered an authorized command in the MD-CLI.
Effect	The CLI command was processed in the MD-CLI engine.
Recovery	No recovery is required.

70.21 md_cli_unauth_io

Table 1327: md_cli_unauth_io properties

Property name	Value
Application name	SECURITY
Event ID	2224

Property name	Value
Event name	md_cli_unauth_io
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	Possible messages: • User *$userName$* from *$srcAddr$* [session ID *$sessionId$*]. Command not allowed for this user: *$command$* • User *$userName$* from *$srcAddr$* [session ID *$sessionId$*]. Command not allowed for this user: *$prompt$ $command$*
Cause	The user entered an unauthorized command in the MD-CLI.
Effect	The MD-CLI command was not processed.
Recovery	No recovery is required.

70.22 netconf_auth

Table 1328: netconf_auth properties

Property name	Value
Application name	SECURITY
Event ID	2227
Event name	netconf_auth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC authorized
Cause	The user called an authorized RPC in the NETCONF interface.
Effect	The RPC was processed.
Recovery	No recovery is required.

70.23 netconf_unauth

Table 1329: netconf_unauth properties

Property name	Value
Application name	SECURITY
Event ID	2228
Event name	netconf_unauth
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	User *$userName$* from *$srcAddr$* port *$srcPort$* to port *$dstPort$* session *$sessionId$*: *$rpcName$* RPC unauthorized
Cause	The user called an unauthorized RPC in the NETCONF interface.
Effect	The RPC was not processed.
Recovery	No recovery is required.

70.24 netconf_user_login

Table 1330: 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
Source stream	security
Message format string	User *$userName$* from *$srcAddr$* logged in

Property name	Value
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required

70.25 netconf_user_login_failed

Table 1331: 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
Source stream	security
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

70.26 netconf_user_login_max_attempts

Table 1332: netconf_user_login_max_attempts properties

Property name	Value
Application name	SECURITY
Event ID	2124

Property name	Value
Event name	netconf_user_login_max_attempts
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.55
Default severity	minor
Source stream	security
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.

70.27 netconf_user_logout

Table 1333: netconf_user_logout properties

Property name	Value
Application name	SECURITY
Event ID	2122
Event name	netconf_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Source stream	security
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

70.28 radiusInetServerOperStatusChange

Table 1334: 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
Source stream	security
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.

70.29 radiusOperStatusChange

Table 1335: radiusOperStatusChange properties

Property name	Value
Application name	SECURITY
Event ID	2014
Event name	radiusOperStatusChange
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.7
Default severity	minor
Source stream	security
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.

70.30 radiusSystemIpAddrNotSet

Table 1336: radiusSystemIpAddrNotSet properties

Property name	Value
Application name	SECURITY
Event ID	2016
Event name	radiusSystemIpAddrNotSet
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	security
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.

Property name	Value
Recovery	Configure the system IP address.

70.31 radiusUserProfileInvalid

Table 1337: radiusUserProfileInvalid properties

Property name	Value
Application name	SECURITY
Event ID	2220
Event name	radiusUserProfileInvalid
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
Message format string	Invalid *$attrType$* '*$attrValue$*' received from RADIUS server for user '*$userName$*'
Cause	The RADIUS server provided invalid user profile entry.
Effect	The RADIUS user will not be authorized to execute any commands.
Recovery	The RADIUS server configuration needs to be updated to contain only valid user profile entries.

70.32 sapDcpDynamicConform

Table 1338: sapDcpDynamicConform properties

Property name	Value
Application name	SECURITY
Event ID	2059
Event name	sapDcpDynamicConform
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.46

Property name	Value
Default severity	warning
Source stream	security
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.

70.33 sapDcpDynamicEnforceAlloc

Table 1339: 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
Source stream	security
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.

70.34 sapDcpDynamicEnforceFreed

Table 1340: 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
Source stream	security
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.

70.35 sapDcpDynamicExcd

Table 1341: 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
Source stream	security
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.

70.36 sapDcpDynamicHoldDownEnd

Table 1342: sapDcpDynamicHoldDownEnd properties

Property name	Value
Application name	SECURITY

Property name	Value
Event ID	2057
Event name	sapDcpDynamicHoldDownEnd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.44
Default severity	warning
Source stream	security
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.

70.37 sapDcpDynamicHoldDownStart

Table 1343: 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
Source stream	security
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$*

Property name	Value
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.

70.38 sapDcpLocMonExcd

Table 1344: 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
Source stream	security
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 dynamic 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.

70.39 sapDcpLocMonExcdAllDynAlloc

Table 1345: 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
Source stream	security
Message format string	All dynamic policers allocated for local monitor *$sapDcpFpLocMonPlcrName$* for sap *$sapEncapValue$* on fp *$tmnxCardSlotNum$/$tmnxFPNum$* at *$sapDcpTimeEventOccured$*. Policy *$sapDCpuProtPolicy$*. 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.

70.40 sapDcpLocMonExcdAllDynFreed

Table 1346: sapDcpLocMonExcdAllDynFreed properties

Property name	Value
Application name	SECURITY
Event ID	2063
Event name	sapDcpLocMonExcdAllDynFreed

Property name	Value
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.50
Default severity	warning
Source stream	security
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.
Recovery	There is no recovery required for this notification.

70.41 sapDcpLocMonExcdDynResource

Table 1347: 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
Source stream	security
Message format string	Local monitor *$sapDcpFpLocMonPlcrName$* for sap *$sapEncap Value$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* detected as non-conformant at *$sapDcpTimeEventOccured$* and cannot allocate

Property name	Value
	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).

70.42 sapDcpStaticConform

Table 1348: 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
Source stream	security
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

Property name	Value
	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.

70.43 sapDcpStaticExcd

Table 1349: 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
Source stream	security
Message format string	Non conformant sap *$sapEncapValue$* on fp *$tmnxCardSlotNum $*/*$tmnxFPNum$* detected at *$sapDcpTimeEventOccured$*. Policy *$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.

70.44 sapDcpStaticHoldDownEnd

Table 1350: 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
Source stream	security
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.

70.45 sapDcpStaticHoldDownStart

Table 1351: sapDcpStaticHoldDownStart properties

Property name	Value
Application name	SECURITY
Event ID	2054
Event name	sapDcpStaticHoldDownStart
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.41

Property name	Value
Default severity	warning
Source stream	security
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.

70.46 ssh_auth_key_gen

Table 1352: ssh_auth_key_gen properties

Property name	Value
Application name	SECURITY
Event ID	2252
Event name	ssh_auth_key_gen
SNMP notification prefix and OID	N/A
Default severity	indeterminate
Source stream	security
Message format string	ssh authentication key generated by user *$userName$* and stored in *$dstPath$*
Cause	A user generated a pair of private and public authentication keys for SSH.
Effect	Generated keys are stored in the compact flash of the active CPM and can be used to authenticate an SSH session to a remote host.
Recovery	No recovery is required

70.47 ssh_auth_key_synch_fail

Table 1353: ssh_auth_key_synch_fail properties

Property name	Value
Application name	SECURITY
Event ID	2253
Event name	ssh_auth_key_synch_fail
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	security
Message format string	failed to synchronize to the standby CPM the ssh authentication key stored in *$dstPath$*
Cause	Synchronization of an SSH authentication key to the standby CPM failed.
Effect	Following a switchover the SSH authentication key may no longer be available to authenticate an SSH session to a remote host.
Recovery	No recovery is required

70.48 SSH_server_preserve_key_fail

Table 1354: 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
Source stream	security

Property name	Value
Message format string	Persistence of SSH server host key failed on *$tmnxCpmFlashHwIndex $* with operational status *$tmnxCpmFlashOperStatus$*.
Cause	Persistence of the SSH server host keys failed.
Effect	The SSH server host key will differ after reboot. The remote server host key will not be stored across reboots.
Recovery	N/A

70.49 ssh_user_login

Table 1355: 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
Source stream	security
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

70.50 ssh_user_login_failed

Table 1356: ssh_user_login_failed properties

Property name	Value
Application name	SECURITY

Property name	Value
Event ID	2011
Event name	ssh_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
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

70.51 ssh_user_login_max_attempts

Table 1357: 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
Source stream	security
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

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 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.
Effect	The user is locked out for a period of tmnxPasswordAttemptsLockoutPeriod minutes. An SSH session is terminated.
Recovery	No recovery action is required.

70.52 ssh_user_logout

Table 1358: 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
Source stream	security
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.

70.53 sysDNSSecFailedAuthentication

Table 1359: 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
Source stream	security
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)'.
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.

70.54 tacplusInetSrvrOperStatusChange

Table 1360: 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

Property name	Value
Source stream	security
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.

70.55 tacplusOperStatusChange

Table 1361: 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
Source stream	security
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.

70.56 tmnxAppPkiCertVerificationFailed

Table 1362: tmnxAppPkiCertVerificationFailed properties

Property name	Value
Application name	SECURITY
Event ID	2116
Event name	tmnxAppPkiCertVerificationFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.54
Default severity	minor
Source stream	security
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.

70.57 tmnxCAProfileStateChange

Table 1363: tmnxCAProfileStateChange properties

Property name	Value
Application name	SECURITY
Event ID	2045
Event name	tmnxCAProfileStateChange
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.18
Default severity	minor
Source stream	security
Message format string	CA profile *$tmnxPkiCAProfile$* changed state to *$tmnxPkiCAProfile OperState$ $tmnxSecNotifFailureReason$*

Property name	Value
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.

70.58 tmnxCAProfUpDueToRevokeChkCrlOpt

Table 1364: 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
Source stream	security
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.

70.59 tmnxCertExport

Table 1365: 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
Source stream	security
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

70.60 tmnxCertImport

Table 1366: 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
Source stream	security
Message format string	admin certificate import type *$tmnxSecNotifyImportExportType$* input *$tmnxSecNotifyUrl$* output *$tmnxSecNotifFile$* format *$tmnxSecNotifyImportExportFormat$* : *$tmnxSecEventOutcome$*

Property name	Value
Cause	A tmnxCertImport notification is generated when a user imports a cryptographic key, certificate, or CRL with the admin certificate command
Effect	N/A
Recovery	N/A

70.61 tmnxCertKeyPairGen

Table 1367: 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
Source stream	security
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

70.62 tmnxCliGroupSessionLimitExceeded

Table 1368: tmnxCliGroupSessionLimitExceeded properties

Property name	Value
Application name	SECURITY
Event ID	2112
Event name	tmnxCliGroupSessionLimitExceeded
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.44
Default severity	minor
Source stream	security
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 privileges) 4) revoke the session group membership for the particular profile

70.63 tmnxConfigCreate

Table 1369: tmnxConfigCreate properties

Property name	Value
Application name	SECURITY

Property name	Value
Event ID	2207
Event name	tmnxConfigCreate
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9
Default severity	warning
Source stream	security
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

70.64 tmnxConfigDelete

Table 1370: 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
Source stream	security
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are

Property name	Value
	committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

70.65 tmnxConfigModify

Table 1371: tmnxConfigModify properties

Property name	Value
Application name	SECURITY
Event ID	2206
Event name	tmnxConfigModify
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.8
Default severity	warning
Source stream	security
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

70.66 tmnxCpmProtDefPolModified

Table 1372: 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
Source stream	security
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.

70.67 tmnxCpmProtExcdSapEcm

Table 1373: tmnxCpmProtExcdSapEcm properties

Property name	Value
Application name	SECURITY
Event ID	2041
Event name	tmnxCpmProtExcdSapEcm
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.14
Default severity	warning
Source stream	security
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,

Property name	Value
	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.

70.68 tmnxCpmProtExcdSapIp

Table 1374: 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
Source stream	security
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::sapCpm ProtMonitorIP to 'false'.
Effect	N/A
Recovery	N/A

70.69 tmnxCpmProtExcdSdpBind

Table 1375: 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
Source stream	security
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.

70.70 tmnxCpmProtExcdSdpBindEcm

Table 1376: tmnxCpmProtExcdSdpBindEcm properties

Property name	Value
Application name	SECURITY
Event ID	2042
Event name	tmnxCpmProtExcdSdpBindEcm
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.15

Property name	Value
Default severity	warning
Source stream	security
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.

70.71 tmnxCpmProtExcdSdpBindIp

Table 1377: 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
Source stream	security
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

Property name	Value
	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.

70.72 tmnxCpmProtViolIf

Table 1378: 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
Source stream	security
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.

70.73 tmnxCpmProtViolIfOutProf

Table 1379: 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
Source stream	security
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.

70.74 tmnxCpmProtViolMac

Table 1380: tmnxCpmProtViolMac properties

Property name	Value
Application name	SECURITY
Event ID	2032
Event name	tmnxCpmProtViolMac
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.7

Property name	Value
Default severity	warning
Source stream	security
Message format string	Per-source packet arrival rate exceeded for MAC *$tmnxCpmProt ViolMacAddress$* SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
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.

70.75 tmnxCpmProtViolPort

Table 1381: 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
Source stream	security
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

Property name	Value
	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.

70.76 tmnxCpmProtViolPortAgg

Table 1382: 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
Source stream	security
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.

70.77 tmnxCpmProtViolSap

Table 1383: 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
Source stream	security
Message format string	Overall packet arrival rate exceeded for SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPkt HexDump$*
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.

70.78 tmnxCpmProtViolSapOutProf

Table 1384: 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
Source stream	security
Message format string	Out-of-Profile control packets rate exceeded for SAP *$sapEncapValue$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcdPktHexDump$*
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.

70.79 tmnxCpmProtViolSdpBind

Table 1385: 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
Source stream	security

Property name	Value
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.

70.80 tmnxCpmProtViolSdpBindOutProf

Table 1386: 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
Source stream	security
Message format string	Out-of-Profile control packets rate exceeded for SDP Bind *$sdpBindId$* in service *$svcId$*. Hex Dump(First 64 bytes): *$tmnxCpmProtViolExcd PktHexDump$*
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.

70.81 tmnxCpmProtViolVdoSvcClient

Table 1387: 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
Source stream	security
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

70.82 tmnxCpmProtViolVdoVrtrClient

Table 1388: tmnxCpmProtViolVdoVrtrClient properties

Property name	Value
Application name	SECURITY
Event ID	2034
Event name	tmnxCpmProtViolVdoVrtrClient
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.9
Default severity	warning
Source stream	security

Property name	Value
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

70.83 tmnxDcpCardFpEventOvrflw

Table 1389: 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
Source stream	security
Message format string	Distributed CPU Protection FP log event overflow occurred on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEventOccured$*
Cause	The tmnxDcpCardFpEventOvrflw notification is generated when a flood of distributed 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.

70.84 tmnxDcpCardFpEventOvrflwClr

Table 1390: 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
Source stream	security
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 distributed 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.

70.85 tmnxDcpCardSapEventOvrflw

Table 1391: 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
Source stream	security
Message format string	Distributed CPU Protection SAP log event overflow occurred on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEventOccured$*

Property name	Value
Cause	The tmnxDcpCardSapEventOvrflw notification is generated when a flood of distributed 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.

70.86 tmnxDcpCardSapEventOvrflwClr

Table 1392: 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
Source stream	security
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 distributed 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.

70.87 tmnxDcpCardVrtrIfEventOvrflw

Table 1393: 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
Source stream	security
Message format string	Distributed CPU Protection Network_if log event overflow occurred on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEvent Occured$*
Cause	The tmnxDcpCardVrtrIfEventOvrflw notification is generated when a flood of distributed 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.

70.88 tmnxDcpCardVrtrIfEventOvrflwClr

Table 1394: 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
Source stream	security
Message format string	*$tmnxDcpMissingNotificationCount$* Distributed CPU Protection Netwk_if log events were dropped in the last event throttling interval

Property name	Value
	on card *$tmnxChassisNotifyCardSlotNum$* at *$tmnxDcpTimeEvent Occured$*
Cause	The tmnxDcpCardVrtrIfEventOvrflwClr notification is generated the when event throttling has ended for distributed CPU protection network-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.

70.89 tmnxDcpFpDynPoolUsageHiAlmClear

Table 1395: 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
Source stream	security
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.

70.90 tmnxDcpFpDynPoolUsageHiAlmRaise

Table 1396: 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
Source stream	security
Message format string	Dynamic Enforcement Pool nearly (or fully) exhausted on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$tmnxDcpTimeEventOccured$*
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.

70.91 tmnxFileCopied

Table 1397: 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
Source stream	security
Message format string	File *$tmnxSecNotifyUrl$* copy to *$tmnxSecNotifyNewUrl$* : *$tmnxSecEventOutcome$*

Property name	Value
Cause	A tmnxFileCopied notification is generated when a user copies a file through the file command
Effect	N/A
Recovery	N/A

70.92 tmnxFileDeleted

Table 1398: 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
Source stream	security
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

70.93 tmnxFileMoved

Table 1399: tmnxFileMoved properties

Property name	Value
Application name	SECURITY
Event ID	2235

Property name	Value
Event name	tmnxFileMoved
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.60
Default severity	minor
Source stream	security
Message format string	File *$tmnxSecNotifyUrl$* move to *$tmnxSecNotifyNewUrl$* : *$tmnxSecEventOutcome$*
Cause	A tmnxFileMoved notification is generated when a user moves a file through the file command
Effect	N/A
Recovery	N/A

70.94 tmnxFileUnzip

Table 1400: tmnxFileUnzip properties

Property name	Value
Application name	SECURITY
Event ID	2237
Event name	tmnxFileUnzip
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.62
Default severity	minor
Source stream	security
Message format string	File unzip operation completed with source *$tmnxSecNotifyUrl$* destination *$tmnxSecNotifyDestUrl$* and result *$tmnxSecNotifFileUnzipResult$*
Cause	The tmnxFileUnzip notification is generated upon the completion of an unzip operation of the source ZIP file specified by tmnxSecNotifyUrl to the destination location specified by tmnxSecNotifyDestUrl.
Effect	The result is indicated by the value of tmnxSecNotifFileUnzipResult as follows: success (0) - unzip is successful. partialSuccess (1) - unzip is partially successful, skipped some files. sourceNotFound (2) - failed - cannot find the ZIP file. sourceNotSupported (3) - failed - ZIP file is not

Property name	Value
	supported. destNotFound (4) - failed - cannot find the destination URL. destFull (5) - failed - destination storage is full. fileTooBig (6) - failed - file size exceeds limit. otherFailure (7) - failed - another reason.
Recovery	No recovery action if tmnxSecNotifFileUnzipResult is success (0). Otherwise, depending on the indicated failure, corrective action should be taken before attempting another unzip operation.

70.95 tmnxKeyChainAuthFailure

Table 1401: tmnxKeyChainAuthFailure properties

Property name	Value
Application name	SECURITY
Event ID	2027
Event name	tmnxKeyChainAuthFailure
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.2
Default severity	minor
Source stream	security
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.

70.96 tmnxMD5AuthFailure

Table 1402: 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
Source stream	security
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.

70.97 tmnxPasswordHashingChanged

Table 1403: 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
Source stream	security
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

Property name	Value
	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.

70.98 tmnxPkiCAProfActnStatusChg

Table 1404: 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
Source stream	security
Message format string	*$tmnxPkiCAProfActnType$* for ca-profile (*$tmnxPkiCAProfile$*) *$tmnx PkiCAProfActnStatus$*. ca-response: *$tmnxCAProfActnStatusCode$*. *$tmnxPkiCAProfActnStatusString$*
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.

70.99 tmnxPkiCAProfCrlUpdAllUrlsFail

Table 1405: 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
Source stream	security
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.

70.100 tmnxPkiCAProfCrlUpdateStart

Table 1406: 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
Source stream	security
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.

70.101 tmnxPkiCAProfCrlUpdateSuccess

Table 1407: 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
Source stream	security
Message format string	A CRL file was successfully updated from *$tmnxPkiCAProfUrl$* (*$tmnx PkiCAProfUrlId$*) for CA profile *$tmnxPkiCAProfile$*

Property name	Value
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.
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.

70.102 tmnxPkiCAProfCrlUpdateUrlFail

Table 1408: 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
Source stream	security
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.

70.103 tmnxPkiCAProfCrlUpdLargPreUpdTm

Table 1409: 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
Source stream	security
Message format string	The CRL pre-update time for CA profile *$tmnxPkiCAProfileNameForNotify$* 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 tmnxPkiCAProfAtCrlUpdAdminState to 'inService (2)' plus the pre-update time. The last successful update time is stored in tmnxPkiCAProfAtCrlUpdLstSucsTmSt. The pre-update time is configured via tmnxPkiCAProfAtCrlUpdPreUpdTime.
Effect	The system will update the CRL again in tmnxPkiCAProfAtCrlUpdRetryIntv 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)'.

70.104 tmnxPkiCAProfCrlUpdNoNxtUpdTime

Table 1410: tmnxPkiCAProfCrlUpdNoNxtUpdTime properties

Property name	Value
Application name	SECURITY
Event ID	2110
Event name	tmnxPkiCAProfCrlUpdNoNxtUpdTime
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.42
Default severity	minor
Source stream	security
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)'.

70.105 tmnxPkiCAProfRevokeChkWarning

Table 1411: tmnxPkiCAProfRevokeChkWarning properties

Property name	Value
Application name	SECURITY
Event ID	2093
Event name	tmnxPkiCAProfRevokeChkWarning
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	minor
Source stream	security
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.
Recovery	Check the value of tmnxPkiCAProfRevokeChk object for this CA profile if it is not expected.

70.106 tmnxPkiCertAfterExpWarning

Table 1412: 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
Source stream	security
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.

70.107 tmnxPkiCertBeforeExpWarning

Table 1413: 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
Source stream	security
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.

70.108 tmnxPkiCertChainCompareCaNoMatch

Table 1414: tmnxPkiCertChainCompareCaNoMatch properties

Property name	Value
Application name	SECURITY
Event ID	2251
Event name	tmnxPkiCertChainCompareCaNoMatch
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.74
Default severity	minor

Property name	Value
Source stream	main
Message format string	Compute chain for certificate file '*$tmnxPkiCertFileNameNotif$*': No chain contains certificate with subject DN ' *$tmnxPkiCertSubjectNotif$*', serial '*$tmnxPkiCertSerialNumberNotif$*'. Returning the first valid chain.
Cause	The tmnxPkiCertChainCompareCaNoMatch notification is generated when a compute chain for a certificate file does not include the expected (configured) CA.
Effect	The first valid chain was selected.
Recovery	Check compare chain include CA configuration (tIPsecCertProfEntry IdCompChainCa).

70.109 tmnxPkiCertExpWarningCleared

Table 1415: 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
Source stream	security
Message format string	Expiration warning for certificate *$tmnxSecNotifFile$* used by *$tmnx SecNotifClientAppName$* 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.

70.110 tmnxPkiCertNotYetValid

Table 1416: 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
Source stream	security
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.

70.111 tmnxPkiCertUpdUpdateFailed

Table 1417: tmnxPkiCertUpdUpdateFailed properties

Property name	Value
Application name	SECURITY
Event ID	2247
Event name	tmnxPkiCertUpdUpdateFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.72

Property name	Value
Default severity	minor
Source stream	security
Message format string	Certificate file: *$tmnxPkiCertUpdCertFileNameNotif$* - Update failed - Reason: *$tmnxPkiCertUpdFailureReasonNotif$*
Cause	The tmnxPkiCertUpdUpdateStarted notification is sent when an X509 certificate update fails.
Effect	The certificate was not updated. Update attempts will continually repeat if the failure was caused by an external server.
Recovery	Check certificate update profile and auto update configuration and attempt to update again.

70.112 tmnxPkiCertUpdUpdateFinished

Table 1418: tmnxPkiCertUpdUpdateFinished properties

Property name	Value
Application name	SECURITY
Event ID	2246
Event name	tmnxPkiCertUpdUpdateFinished
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.71
Default severity	minor
Source stream	security
Message format string	Certificate file: *$tmnxPkiCertUpdCertFileNameNotif$* - Update finished - Serial number: *$tmnxPkiCertUpdSerialNumberNotif$* - Subject: *$tmnxPkiCertUpdSubjectNotif$*
Cause	The tmnxPkiCertUpdUpdateStarted notification is sent when an X509 certificate update finishes.
Effect	The certificate was updated.
Recovery	Check certificate update profile configuration and attempt to update again.

70.113 tmnxPkiCertUpdUpdateStarted

Table 1419: tmnxPkiCertUpdUpdateStarted properties

Property name	Value
Application name	SECURITY
Event ID	2245
Event name	tmnxPkiCertUpdUpdateStarted
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.70
Default severity	minor
Source stream	security
Message format string	Certificate file: *$tmnxPkiCertUpdCertFileNameNotif$* - Update started
Cause	The tmnxPkiCertUpdUpdateStarted notification is sent when an X509 certificate update starts as specified by a tmnxPkiCertUpdProfileName.
Effect	The certificate will attempt to update.
Recovery	No recovery action is required.

70.114 tmnxPkiCertVerificationFailed

Table 1420: 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
Source stream	security
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.

70.115 tmnxPkiCRLAfterExpWarning

Table 1421: 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
Source stream	security
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).

70.116 tmnxPkiCRLBeforeExpWarning

Table 1422: tmnxPkiCRLBeforeExpWarning properties

Property name	Value
Application name	SECURITY
Event ID	2098
Event name	tmnxPkiCRLBeforeExpWarning
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.31
Default severity	minor
Source stream	security
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).

70.117 tmnxPkiCRLExpWarningCleared

Table 1423: 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
Source stream	security
Message format string	Expiration warning for CRL *$tmnxSecNotifFile$* is no longer applicable because of the following reason: *$tmnxPkiExpReason$*

Property name	Value
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.

70.118 tmnxPkiCRLNotYetValid

Table 1424: 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
Source stream	security
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.

70.119 tmnxPkiFileReadFailed

Table 1425: 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
Source stream	security
Message format string	File *$tmnxSecNotifFile$* read failed due to *$tmnxSecNotifFailure Reason$*
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.

70.120 tmnxPkiFileWriteFailed

Table 1426: 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

Property name	Value
Source stream	security
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 writable and there is sufficient disk space.

70.121 tmnxSecComputeCertChainFailure

Table 1427: tmnxSecComputeCertChainFailure properties

Property name	Value
Application name	SECURITY
Event ID	2088
Event name	tmnxSecComputeCertChainFailure
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.24
Default severity	warning
Source stream	security
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 occurred.
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.

70.122 tmnxSecNotifFileReloaded

Table 1428: 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
Source stream	security
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.

70.123 tmnxSecNotifKeyChainExpired

Table 1429: 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
Source stream	security

Property name	Value
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

70.124 tmnxSecPwdHistoryFileLoadFailed

Table 1430: tmnxSecPwdHistoryFileLoadFailed properties

Property name	Value
Application name	SECURITY
Event ID	2103
Event name	tmnxSecPwdHistoryFileLoadFailed
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.35
Default severity	minor
Source stream	main
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 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.

70.125 tmnxSecPwdHistoryFileWriteFailed

Table 1431: 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
Source stream	main
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.

70.126 tmnxSecSignedSwCpmBootEvent

Table 1432: tmnxSecSignedSwCpmBootEvent properties

Property name	Value
Application name	SECURITY
Event ID	2241
Event name	tmnxSecSignedSwCpmBootEvent
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.66
Default severity	major

Property name	Value
Source stream	main
Message format string	CPM *$tmnxChassisNotifyCpmCardSlotNum$* has booted with a secure-boot status of *$tmnxCpmSecureBootEnabled$*
Cause	The tmnxSecSignedSwCpmBootEvent is sent when a CPM element reboots, regardless of its secure boot configuration. The event will include relevant information about the state of secure boot on the CPM.
Effect	The indicated CPM has rebooted.
Recovery	No recovery action is required.

70.127 tmnxSecSignedSwImgValFail

Table 1433: tmnxSecSignedSwImgValFail properties

Property name	Value
Application name	SECURITY
Event ID	2243
Event name	tmnxSecSignedSwImgValFail
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.68
Default severity	major
Source stream	main
Message format string	The signed software image located at *$tmnxSecureBootValdImgUrl$*, for CPM *$tmnxChassisNotifyCpmCardSlotNum$*, failed to be validated. As a result, the CPM will not boot
Cause	The tmnxSecSignedSwImgValFail notification is sent when the secure boot validation process fails for any reason to approve an image at a given URL. This event is only applicable to CPMs with secure boot enabled.
Effect	The affected CPM will not boot.
Recovery	The CPM should be examined for availability and correct configuration of its signed software image(s). A reboot will be required to attempt to validate the software again.

70.128 tmnxSSHListeningPortChanged

Table 1434: tmnxSSHListeningPortChanged properties

Property name	Value
Application name	SECURITY
Event ID	2254
Event name	tmnxSSHListeningPortChanged
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.75
Default severity	minor
Source stream	main
Message format string	User *$tmnxSecNotifyUserName$* has changed the SSH port to *$tmnxSSHListeningPort$*
Cause	The tmnxSSHListeningPortChanged notification is generated when the TCP port which the SSH server listens on is changed.
Effect	SSH server port is changed.
Recovery	No recovery action is required.

70.129 tmnxSSHListeningPortInUse

Table 1435: tmnxSSHListeningPortInUse properties

Property name	Value
Application name	SECURITY
Event ID	2258
Event name	tmnxSSHListeningPortInUse
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.79
Default severity	minor
Source stream	main

Property name	Value
Message format string	Application is trying to open a connection on SSH port *$tmnxSSHListeningPort$*
Cause	The tmnxSSHListeningPortInUse notification is generated when a TCP port cannot be configured because it is already in use when another application attempts to connect to the port currently used by the SSH server.
Effect	The TCP port has not been changed.
Recovery	No recovery action is required.

70.130 tmnxSSHListeningPortOccupied

Table 1436: tmnxSSHListeningPortOccupied properties

Property name	Value
Application name	SECURITY
Event ID	2256
Event name	tmnxSSHListeningPortOccupied
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.77
Default severity	minor
Source stream	main
Message format string	SSH port *$tmnxSSHListeningPort$* cannot be configured because this port is used by another application
Cause	The tmnxSSHListeningPortOccupied notification is generated when a TCP port cannot be configured because it is already occupied by another application when the SSH server attempts to access the port.
Effect	SSH server port is not changed.
Recovery	No recovery action is required.

70.131 tmnxSSHSessionFailed

Table 1437: tmnxSSHSessionFailed properties

Property name	Value
Application name	SECURITY
Event ID	2240
Event name	tmnxSSHSessionFailed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	security
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.

70.132 tmnxStateChange

Table 1438: 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
Source stream	security

Property name	Value
Message format string	Status of *$tmnxNotifyObjectName$* changed administrative state: *$tmnxNotifyRowAdminState$*, operational state: *$tmnxNotifyRowOperState$*
Cause	There was a change in either the administrative or operational state of a MIB table entry.
Effect	N/A
Recovery	No recovery is necessary.

70.133 tmnxSysAppLicenseInsufficient

Table 1439: tmnxSysAppLicenseInsufficient properties

Property name	Value
Application name	SECURITY
Event ID	2225
Event name	tmnxSysAppLicenseInsufficient
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.81
Default severity	major
Source stream	main
Message format string	License *$tmnxSysAppLicenseState$* for *$tmnxSysLicensingNotifyGroup$* feature ' *$tmnxSysLicensedNotifyAppName$*': *$tmnxSysLicenseErrorReason$*
Cause	The tmnxSysAppLicenseInsufficient notification is generated periodically when licensing for an application is detected to be insufficient. The details of the error is specified in tmnxSysLicenseErrorReason. This notification cannot be suppressed.
Effect	Notification generated periodically while the application remains in this condition.
Recovery	Activate a system license containing sufficient license entitlements for this application.

70.134 tmnxSysLicenseActivated

Table 1440: tmnxSysLicenseActivated properties

Property name	Value
Application name	SECURITY
Event ID	2125
Event name	tmnxSysLicenseActivated
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.75
Default severity	warning
Source stream	security
Message format string	*$tmnxHwIndex$* is running with a valid license.
Cause	The tmnxSysLicenseActivated notification is generated each time a license is activated on the system.
Effect	The system is running with the license specified in tmnxSysLicense Name.
Recovery	No recovery.

70.135 tmnxSysLicenseCleared

Table 1441: tmnxSysLicenseCleared properties

Property name	Value
Application name	SECURITY
Event ID	2249
Event name	tmnxSysLicenseCleared
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.95
Default severity	warning
Source stream	security
Message format string	*$tmnxHwIndex$* is no longer running with a license.

Property name	Value
Cause	The tmnxSysLicenseCleared notification is generated each time a license is cleared from the system.
Effect	The system is no longer running with a license.
Recovery	No recovery.

70.136 tmnxSysLicenseExpiresSoon

Table 1442: 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
Source stream	security
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.

70.137 tmnxSysLicenseInvalid

Table 1443: tmnxSysLicenseInvalid properties

Property name	Value
Application name	SECURITY

Property name	Value
Event ID	2091
Event name	tmnxSysLicenseInvalid
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.59
Default severity	major
Source stream	security
Message format string	Error - *$tmnxSysLicenseErrorReason$* record. *$tmnxHwIndex$* will *$tmnxSysLicenseErrorAction$ $tmnxSysLicenseTimeLeft$*.
Cause	Generated when the license becomes invalid for the reason specified in tmnxSysLicenseErrorReason.
Effect	The CPM or system will reboot at the end of the time remaining, as specified by tmnxSysLicenseTimeLeft and tmnxSysLicenseErrorAction.
Recovery	Configure a valid license file location and file name, given the value of tmnxSysLicenseErrorReason.

70.138 tmnxSysLicenseUpdateRequired

Table 1444: tmnxSysLicenseUpdateRequired properties

Property name	Value
Application name	SECURITY
Event ID	2226
Event name	tmnxSysLicenseUpdateRequired
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.84
Default severity	major
Source stream	security
Message format string	System license update is required.
Cause	The tmnxSysLicenseUpdateRequired notification is generated once after the system boots up and the license is determined by the system to be valid, but requires to be updated to the correct software version.
Effect	The system will use the license until it is updated.

Property name	Value
Recovery	Update and activate the updated license.

70.139 tmnxSysLicenseValid

Table 1445: 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
Source stream	security
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.

70.140 tmnxSysLicensingStateOk

Table 1446: tmnxSysLicensingStateOk properties

Property name	Value
Application name	SECURITY
Event ID	2250
Event name	tmnxSysLicensingStateOk

Property name	Value
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.96
Default severity	warning
Source stream	security
Message format string	*$tmnxHwIndex$* no longer has licensing violations.
Cause	The tmnxSysLicensingStateOk notification is generated when all licensing violations have been cleared from the system.
Effect	The system no longer has any licensing violations.
Recovery	No recovery.

70.141 tmnxSysStandbyLicensingError

Table 1447: tmnxSysStandbyLicensingError properties

Property name	Value
Application name	SECURITY
Event ID	2221
Event name	tmnxSysStandbyLicensingError
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.76
Default severity	major
Source stream	main
Message format string	*$tmnxHwIndex$* is not licensed. *$tmnxSysLicenseErrorReason$*.
Cause	Generated when the standby detects a licensing failure. The reason is specified in tmnxSysLicenseErrorReason.
Effect	The standby CPM may not synchronized and may be put into a failed state.
Recovery	Configure a valid license file location and file name, given the value of tmnxSysLicenseErrorReason.

70.142 tmnxSysStandbyLicensingReady

Table 1448: tmnxSysStandbyLicensingReady properties

Property name	Value
Application name	SECURITY
Event ID	2222
Event name	tmnxSysStandbyLicensingReady
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.77
Default severity	warning
Source stream	main
Message format string	*$tmnxHwIndex$* licensing is ready.
Cause	Generated when licensing has been successfully activated by the standby.
Effect	Any licensing errors detected by the Standby CPM are cleared.
Recovery	None.

70.143 tmnxSysSwDSValidationResult

Table 1449: tmnxSysSwDSValidationResult properties

Property name	Value
Application name	SECURITY
Event ID	2260
Event name	tmnxSysSwDSValidationResult
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.97
Default severity	minor
Source stream	security

Property name	Value
Message format string	Software location *$tmnxSysSwDSValidationIndex$* at *$tmnxSys SwDSValidationUrl$* digital signature state is *$tmnxSysSwDSValidation State$*.
Cause	A software digital signature validation has completed.
Effect	N/A
Recovery	No recovery is necessary.

70.144 tmnxSystemPasswordChangedByAdmin

Table 1450: 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
Source stream	security
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.

70.145 tmnxTelnetListeningPortChanged

Table 1451: tmnxTelnetListeningPortChanged properties

Property name	Value
Application name	SECURITY
Event ID	2255
Event name	tmnxTelnetListeningPortChanged
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.76
Default severity	minor
Source stream	main
Message format string	User *$tmnxSecNotifyUserName$* has changed the Telnet port to *$tmnx TelnetListeningPort$*
Cause	The tmnxTelnetListeningPortChanged notification is generated when the TCP port which the Telnet server listens on is changed.
Effect	Telnet server port is changed.
Recovery	No recovery action is required.

70.146 tmnxTelnetListeningPortInUse

Table 1452: tmnxTelnetListeningPortInUse properties

Property name	Value
Application name	SECURITY
Event ID	2259
Event name	tmnxTelnetListeningPortInUse
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.80
Default severity	minor
Source stream	main

Property name	Value
Message format string	Application is trying to open a connection on Telnet port *$tmnxTelnet ListeningPort$*
Cause	The tmnxTelnetListeningPortInUse notification is generated when a TCP port cannot be configured because it is already in use when another application attempts to connect to the port currently used by the Telnet server.
Effect	The TCP port has not been changed.
Recovery	No recovery action is required.

70.147 tmnxTelnetListeningPortOccupied

Table 1453: tmnxTelnetListeningPortOccupied properties

Property name	Value
Application name	SECURITY
Event ID	2257
Event name	tmnxTelnetListeningPortOccupied
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.78
Default severity	minor
Source stream	main
Message format string	Telnet port *$tmnxTelnetListeningPort$* cannot be configured because this port is used by another application
Cause	The tmnxTelnetListeningPortOccupied notification is generated when a TCP port cannot be configured because it is already occupied by another application when the Telnet server attempts to access the port.
Effect	Telnet server port is not changed.
Recovery	No recovery action is required.

70.148 tmnxUserPasswordChangedByAdmin

Table 1454: 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
Source stream	security
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.

70.149 tmnxUsrProfSessionLimitExceeded

Table 1455: 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
Source stream	security

Property name	Value
Message format string	*$tmnxSessionLimitExceededType$* of user profile '*$tmnxSessionLimit ExceededName$*' 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 privileges)

70.150 tSecSgndSwUefiVarsUpdtReqd

Table 1456: tSecSgndSwUefiVarsUpdtReqd properties

Property name	Value
Application name	SECURITY
Event ID	2242
Event name	tSecSgndSwUefiVarsUpdtReqd
SNMP notification prefix and OID	TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.67
Default severity	major
Source stream	main
Message format string	UEFI variable updates required for CPM *$tmnxChassisNotifyCpmCard SlotNum$*
Cause	The tSecSgndSwUefiVarsUpdtReqd is sent when a CPM element reboots with UEFI variables which are out of date with the software image that CPM is configured to boot into.

Property name	Value
Effect	Out-of-sync UEFI variables may prevent successful reboots into signed software images and result in warnings or errors during secure-boot operations.
Recovery	The CPM and its target images should be examined and any incorrect secure-boot settings corrected to ensure proper configuration.

70.151 user_disconnect

Table 1457: user_disconnect properties

Property name	Value
Application name	SECURITY
Event ID	2015
Event name	user_disconnect
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	security
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

70.152 vRtrIfDcpDynamicConform

Table 1458: vRtrIfDcpDynamicConform properties

Property name	Value
Application name	SECURITY
Event ID	2073

Property name	Value
Event name	vRtrIfDcpDynamicConform
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.54
Default severity	warning
Source stream	security
Message format string	Network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/ *$tmnxFPNum $* newly conformant at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtr IfDCpuProtPolicy$*. Policer= *$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.

70.153 vRtrIfDcpDynamicEnforceAlloc

Table 1459: 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
Source stream	security

Property name	Value
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.

70.154 vRtrIfDcpDynamicEnforceFreed

Table 1460: 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
Source stream	security
Message format string	Dynamic *$vRtrIfDcpFpProtocol$* policers freed for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. Excd count=*$vRtrIfDcpFpDynExcdCount$*
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'.

Property name	Value
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.

70.155 vRtrIfDcpDynamicExcd

Table 1461: 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
Source stream	security
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.

70.156 vRtrIfDcpDynamicHoldDownEnd

Table 1462: 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
Source stream	security
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.

70.157 vRtrIfDcpDynamicHoldDownStart

Table 1463: vRtrIfDcpDynamicHoldDownStart properties

Property name	Value
Application name	SECURITY
Event ID	2069
Event name	vRtrIfDcpDynamicHoldDownStart

Property name	Value
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.50
Default severity	warning
Source stream	security
Message format string	Hold-down started for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlot Num$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtr IfDCpuProtPolicy$*. 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.

70.158 vRtrIfDcpLocMonExcd

Table 1464: 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
Source stream	security
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

Property name	Value
	attempt to allocate dynamic 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.

70.159 vRtrIfDcpLocMonExcdAllDynAlloc

Table 1465: 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
Source stream	security
Message format string	All dynamic policers allocated for local monitor *$vRtrIfDcpFpLocMon PlcrName$* for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$/ $tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpu ProtPolicy$*. 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.

70.160 vRtrIfDcpLocMonExcdAllDynFreed

Table 1466: 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
Source stream	security
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.

70.161 vRtrIfDcpLocMonExcdDynResource

Table 1467: vRtrIfDcpLocMonExcdDynResource properties

Property name	Value
Application name	SECURITY

Property name	Value
Event ID	2075
Event name	vRtrIfDcpLocMonExcdDynResource
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.56
Default severity	warning
Source stream	security
Message format string	Local monitor *$vRtrIfDcpFpLocMonPlcrName$* for network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/*$tmnxFPNum$* detected as non-conformant at *$vRtrIfDcpTimeEventOccured$* and cannot allocate dynamic policers. Policy *$vRtrIfDCpuProtPolicy$*. Excd count=*$vRtrIfDcpFpLocMonExcdCount$*
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::tmnxDCpuProtLocMonPlcrLogEvent 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 or to the dynamic enforcement policer pool (TIMETRA-CHASSIS-MIB.mib::tmnxFPDCpuProtDynEnfrcPlcrPool).

70.162 vRtrIfDcpStaticConform

Table 1468: vRtrIfDcpStaticConform properties

Property name	Value
Application name	SECURITY
Event ID	2072
Event name	vRtrIfDcpStaticConform
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.53

Property name	Value
Default severity	warning
Source stream	security
Message format string	Network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/ *$tmnxFPNum $* newly conformant at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtr IfDCpuProtPolicy$*. Policer= *$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.

70.163 vRtrIfDcpStaticExcd

Table 1469: 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
Source stream	security
Message format string	Non conformant network_if *$vRtrIfIndex$* on fp *$tmnxCardSlotNum$*/ *$tmnxFPNum$* detected at *$vRtrIfDcpTimeEventOccured$*. Policy *$v RtrIfDCpuProtPolicy$*. 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-

Property name	Value
	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.

70.164 vRtrIfDcpStaticHoldDownEnd

Table 1470: 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
Source stream	security
Message format string	Hold-down completed for network_if *$vRtrIfIndex$* on fp *$tmnxCard SlotNum$*/*$tmnxFPNum$* at *$vRtrIfDcpTimeEventOccured$*. Policy *$vRtrIfDCpuProtPolicy$*. 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.

70.165 vRtrIfDcpStaticHoldDownStart

Table 1471: 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
Source stream	security
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.

71 SFLOW

71.1 tmnxSflowCpEntrySampling

Table 1472: 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
Source stream	main
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

71.2 tmnxSflowPacketTxFailure

Table 1473: tmnxSflowPacketTxFailure properties

Property name	Value
Application name	SFLOW
Event ID	2002
Event name	tmnxSflowPacketTxFailure
SNMP notification prefix and OID	TIMETRA-SFLOW-MIB.tmnxSflowNotifications.2

Property name	Value
Default severity	minor
Source stream	main
Message format string	sFlow failed to send packet to receiver - *$tmnxSflowNotifyFlowFail Reason$*
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

72 SNMP

72.1 authenticationFailure

Table 1474: 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
Source stream	security
Message format string	Request PDU failed authentication for *$subject$*, from IP *$sourceUDP$*
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.

72.2 coldStart

Table 1475: coldStart properties

Property name	Value
Application name	SNMP
Event ID	2001
Event name	coldStart
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.1
Default severity	major
Source stream	main
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 relevant counters to establish a new baseline. Re-poll relevant objects to discover present configuration.

72.3 fallingAlarm

Table 1476: 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
Source stream	main
Message format string	RMON alarm: *$alarmDescription$*

Property name	Value
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

72.4 linkDown

Table 1477: 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
Source stream	main
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.

72.5 linkUp

Table 1478: 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
Source stream	main
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 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.

72.6 risingAlarm

Table 1479: 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
Source stream	main
Message format string	RMON alarm: *$alarmDescription$*

Property name	Value
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

72.7 snmpdError

Table 1480: 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
Source stream	main
Message format string	SNMP Error: *$tmnxSnmpdErrorMsg$*
Cause	The Snmp daemon detected an error.
Effect	N/A
Recovery	N/A

72.8 warmStart

Table 1481: warmStart properties

Property name	Value
Application name	SNMP
Event ID	2002

Property name	Value
Event name	warmStart
SNMP notification prefix and OID	SNMPv2-MIB.snmpTraps.2
Default severity	major
Source stream	main
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 relevant counters to establish a new baseline. There is no need to re-poll relevant objects to discover present configuration.

73 SR_MPLS

73.1 tmnxSrMplsPfxSidFailure

Table 1482: tmnxSrMplsPfxSidFailure properties

Property name	Value
Application name	SR_MPLS
Event ID	2001
Event name	tmnxSrMplsPfxSidFailure
SNMP notification prefix and OID	TIMETRA-SR-MPLS-MIB.tmnxSrNotifications.1
Default severity	warning
Source stream	main
Message format string	Prefix SID *$vRtrIfIndex$* failure: *$tmnxSrMplsNotifyDescription$*
Cause	This notification is generated when the system cannot program the prefix SID due to conflicting configuration of the interface, a duplicate SID or system exhaustion.
Effect	The Segment Routing tunnel will not be programmed and will not be advertised by other protocols
Recovery	In case of system exhaustion, the system will periodically retry. In case of interface configuration conflict or duplicate, the parameters need to be corrected.

73.2 tmnxSrMplsPfxSidFlexAlgoFailure

Table 1483: tmnxSrMplsPfxSidFlexAlgoFailure properties

Property name	Value
Application name	SR_MPLS
Event ID	2002

Property name	Value
Event name	tmnxSrMplsPfxSidFlexAlgoFailure
SNMP notification prefix and OID	TIMETRA-SR-MPLS-MIB.tmnxSrNotifications.2
Default severity	warning
Source stream	main
Message format string	Prefix SID *$vRtrIfIndex$* Flex Algo *$tmnxSrMplsPfxSidFlexAlgoId$* failure: *$tmnxSrMplsNotifyDescription$*
Cause	This notification is generated when the system cannot program the Flex Algo prefix SID due to conflicting configuration of the interface, a duplicate SID or system exhaustion.
Effect	The Segment Routing tunnel will not be programmed and will not be advertised by other protocols
Recovery	In case of system exhaustion, the system will periodically retry. In case of interface configuration conflict or duplicate, the parameters need to be corrected.

74 SRV6

74.1 vRtrSrv6FunctionExhaustion

Table 1484: vRtrSrv6FunctionExhaustion properties

Property name	Value
Application name	SRV6
Event ID	2001
Event name	vRtrSrv6FunctionExhaustion
SNMP notification prefix and OID	TIMETRA-SRV6-MIB.tmnxSrv6Notifications.1
Default severity	minor
Source stream	main
Message format string	Allocation of *$vRtrNotifSrv6ExhaustedRsrc$* failed for router *$vRtrID $ $vRtrNotifSrv6LocatorType$ $vRtrSrv6LocName$* function *$vRtr Srv6FunctionType$* value *$vRtrSrv6FunctionValue$*.
Cause	The vRtrSrv6FunctionExhaustion notification is generated when the function or label allocation fails.
Effect	A log entry is generated.
Recovery	if another entity or local config change returns resources, then it will automatically allocated.

74.2 vRtrSrv6LocatorResExhaustion

Table 1485: vRtrSrv6LocatorResExhaustion properties

Property name	Value
Application name	SRV6
Event ID	2003

Property name	Value
Event name	vRtrSrv6LocatorResExhaustion
SNMP notification prefix and OID	TIMETRA-SRV6-MIB.tmnxSrv6Notifications.3
Default severity	minor
Source stream	main
Message format string	TODO
Cause	The vRtrSrv6LocatorResExhaustion notification is generated when the allocation of locator resources fails.
Effect	A log entry is generated.
Recovery	if another entity or local config change returns resources, then it will automatically allocated.

74.3 vRtrSrv6SvcSidIndex

Table 1486: vRtrSrv6SvcSidIndex properties

Property name	Value
Application name	SRV6
Event ID	2002
Event name	vRtrSrv6SvcSidIndex
SNMP notification prefix and OID	TIMETRA-SRV6-MIB.tmnxSrv6Notifications.2
Default severity	minor
Source stream	main
Message format string	TODO
Cause	The vRtrSrv6SvcSidIndex notification is generated when the service SID index is above or below vRtrSrv6SidIndex.
Effect	A log entry is generated.
Recovery	A config or a policy change to reduce the usage.

75 STP

75.1 higherPriorityBridge

Table 1487: 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
Source stream	main
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.

75.2 newRootBridge

Table 1488: newRootBridge properties

Property name	Value
Application name	STP
Event ID	2007

Property name	Value
Event name	newRootBridge
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.7
Default severity	warning
Source stream	main
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.

75.3 newRootSap

Table 1489: 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
Source stream	main
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.

Property name	Value
Recovery	Check new topology against provisioned topology and determine the severity of connectivity loss.

75.4 newRootVcpState

Table 1490: newRootVcpState properties

Property name	Value
Application name	STP
Event ID	2004
Event name	newRootVcpState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.4
Default severity	warning
Source stream	main
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

75.5 pipActiveProtocolChange

Table 1491: pipActiveProtocolChange properties

Property name	Value
Application name	STP
Event ID	2056

Property name	Value
Event name	pipActiveProtocolChange
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.42
Default severity	minor
Source stream	main
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 vice versa.
Effect	N/A
Recovery	No recovery is necessary.

75.6 receivedTCN

Table 1492: 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
Source stream	main
Message format string	TCN received for service *$svcId$* (customer *$custId$*) on SAP *$sapEncapValue$*
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.

75.7 sapActiveProtocolChange

Table 1493: 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
Source stream	main
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 vice versa.
Effect	N/A
Recovery	No recovery is necessary.

75.8 sapEncapDot1d

Table 1494: 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
Source stream	main

Property name	Value
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.

75.9 sapEncapPVST

Table 1495: 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
Source stream	main
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.
Effect	The SAP STP's BPDUs will be PVST encapsulated.
Recovery	No recovery is needed.

75.10 tmnxNewCistRegionalRootBridge

Table 1496: tmnxNewCistRegionalRootBridge properties

Property name	Value
Application name	STP

Property name	Value
Event ID	2021
Event name	tmnxNewCistRegionalRootBridge
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.33
Default severity	warning
Source stream	main
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.

75.11 tmnxNewMstiRegionalRootBridge

Table 1497: 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
Source stream	main
Message format string	New MSTI regional root *$tlsMstiRegionalRoot$* elected in service *$svc Id$*. Msti-InstanceId: *$svcMstiInstanceId$*
Cause	A STP selected a new regional root for the MSTI.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

75.12 tmnxPipStpExcepCondStateChng

Table 1498: 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
Source stream	main
Message format string	The stp exception condition state for service *$svcId$* (customer *$custId $*) on PIP has changed to *$tlsPipStpException$*
Cause	The STP exception state has changed.
Effect	N/A
Recovery	N/A

75.13 tmnxSapStpExcepCondStateChng

Table 1499: 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
Source stream	main
Message format string	The stp exception condition state for service *$svcId$* (customer *$custId $*) on SAP *$sapEncapValue$* has changed to *$sapTlsStpException$*

Property name	Value
Cause	A STP exception state has changed.
Effect	N/A
Recovery	N/A

75.14 tmnxSdpBndStpExcepCondStateChng

Table 1500: 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
Source stream	main
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

75.15 tmnxStpMeshNotInMstRegion

Table 1501: tmnxStpMeshNotInMstRegion properties

Property name	Value
Application name	STP
Event ID	2024

Property name	Value
Event name	tmnxStpMeshNotInMstRegion
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.36
Default severity	warning
Source stream	main
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.

75.16 tmnxStpRootGuardViolation

Table 1502: 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
Source stream	main
Message format string	A root-guard violation is detected for service *$svcId$* on SAP *$sapEncapValue$*
Cause	A STP detects a root-guard violation.
Effect	The query will be ignored.
Recovery	No recovery is necessary.

75.17 tmnxSvcNewRootSdpBind

Table 1503: tmnxSvcNewRootSdpBind properties

Property name	Value
Application name	STP
Event ID	2015
Event name	tmnxSvcNewRootSdpBind
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.15
Default severity	warning
Source stream	main
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.

75.18 tmnxSvcSdpActiveProtocolChange

Table 1504: 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

Property name	Value
Source stream	main
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 vice versa.
Effect	N/A
Recovery	No recovery is necessary.

75.19 tmnxSvcSdpBindEncapDot1d

Table 1505: 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
Source stream	main
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.

75.20 tmnxSvcSdpBindEncapPVST

Table 1506: 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
Source stream	main
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.

75.21 tmnxSvcSdpBindRcvdHigherBriPrio

Table 1507: 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
Source stream	main
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.

Property name	Value
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.

75.22 tmnxSvcSdpBindRcvdTCN

Table 1508: 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
Source stream	main
Message format string	TCN received for service *$svcId$* (customer *$custId$*) on SDP Bind *$sdpBindId$*
Cause	A SDP Binding has received 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.

75.23 tmnxSvcTopoChgSdpBindMajorState

Table 1509: tmnxSvcTopoChgSdpBindMajorState properties

Property name	Value
Application name	STP

Property name	Value
Event ID	2014
Event name	tmnxSvcTopoChgSdpBindMajorState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.14
Default severity	warning
Source stream	main
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.

75.24 tmnxSvcTopoChgSdpBindState

Table 1510: tmnxSvcTopoChgSdpBindState properties

Property name	Value
Application name	STP
Event ID	2016
Event name	tmnxSvcTopoChgSdpBindState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.16
Default severity	warning
Source stream	main
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.

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.

75.25 topologyChangePipMajorState

Table 1511: 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
Source stream	main
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

75.26 topologyChangePipState

Table 1512: topologyChangePipState properties

Property name	Value
Application name	STP

Property name	Value
Event ID	2054
Event name	topologyChangePipState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.40
Default severity	warning
Source stream	main
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.

75.27 topologyChangeSapMajorState

Table 1513: 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
Source stream	main
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.

75.28 topologyChangeSapState

Table 1514: 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
Source stream	main
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.

75.29 topologyChangeVcpState

Table 1515: topologyChangeVcpState properties

Property name	Value
Application name	STP
Event ID	2003
Event name	topologyChangeVcpState
SNMP notification prefix and OID	TIMETRA-SERV-MIB.tstpTraps.3
Default severity	warning
Source stream	main
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.

75.30 unacknowledgedTCN

Table 1516: 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
Source stream	main
Message format string	TCN sent for service *$svcId$* (customer *$custId$*) to SDP *$sdpId$* is unacknowledged

Property name	Value
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.

75.31 vcpActiveProtocolChange

Table 1517: 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
Source stream	main
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 vice versa.
Effect	N/A
Recovery	No recovery is necessary.

76 SVCMGR

76.1 aluIpTransportStateChanged

Table 1518: aluIpTransportStateChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2573
Event name	aluIpTransportStateChanged
SNMP notification prefix and OID	ALU-IP-TRANSPORT-MIB.aluIpTransportNotifications.1
Default severity	minor
Source stream	main
Message format string	IPT *$aluIpTransportNotifyPortId$* on service *$aluIpTransportNotifySvcId$* changed state to admin=*$aluIpTransportAdminState$* oper=*$aluIpTransportOperState$* flags= *$aluIpTransportOperFlags$*
Cause	This notification may be triggered for a number of reasons, including but not limited to the following: 1) The user has administratively set the IP Transport up or down 2) The access port (or socket) has gone operationally up or down 3) The user has added or removed an IP address from the interface.
Effect	When aluIpTransportOperState indicates outOfService (or down), the IP Transport can no longer carry data over the network.
Recovery	The value of aluIpTransportOperFlags will indicate what needs attention.

76.2 dynamicSdpBindConfigChanged

Table 1519: 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
Source stream	main
Message format string	The configuration for dynamic *$dynamicSdpOrigin$* SDP Bind *$svcL2RteSdpBindId$ $sdpMSPwPeId$* was *$dynamicSdpStatus$*.
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."

76.3 dynamicSdpBindCreationFailed

Table 1520: 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
Source stream	main

Property name	Value
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

76.4 dynamicSdpConfigChanged

Table 1521: dynamicSdpConfigChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2319
Event name	dynamicSdpConfigChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.24
Default severity	major
Source stream	main
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

76.5 dynamicSdpCreationFailed

Table 1522: 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
Source stream	main
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

76.6 hostConnectivityLost

Table 1523: hostConnectivityLost properties

Property name	Value
Application name	SVCMGR
Event ID	2206
Event name	hostConnectivityLost
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.13
Default severity	warning
Source stream	main
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 connectivity with a host.
Effect	N/A

Property name	Value
Recovery	N/A

76.7 hostConnectivityRestored

Table 1524: 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
Source stream	main
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

76.8 iesIfStatusChanged

Table 1525: iesIfStatusChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2108
Event name	iesIfStatusChanged
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.8

Property name	Value
Default severity	minor
Source stream	main
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

76.9 msapCreationFailure

Table 1526: 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
Source stream	main
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

76.10 msapStateChanged

Table 1527: 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
Source stream	main
Message format string	Managed SAP, *$sapEncapValue$* in service *$svcId$*, has been *$msapStatus$*
Cause	A managed SAP was 'created', 'modified', or 'deleted'.
Effect	N/A
Recovery	N/A

76.11 sapCemPacketDefectAlarm

Table 1528: 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
Source stream	main
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

Property name	Value
Recovery	N/A

76.12 sapCemPacketDefectAlarmClear

Table 1529: 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
Source stream	main
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

76.13 sapEthLoopbackStarted

Table 1530: sapEthLoopbackStarted properties

Property name	Value
Application name	SVCMGR
Event ID	2230
Event name	sapEthLoopbackStarted
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.54

Property name	Value
Default severity	minor
Source stream	main
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

76.14 sapEthLoopbackStopped

Table 1531: 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
Source stream	main
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.
Recovery	N/A

76.15 sapHostBGPPeeringSetupFailed

Table 1532: 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
Source stream	main
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 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

76.16 sapHostRipListenerSetupFailed

Table 1533: sapHostRipListenerSetupFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2553
Event name	sapHostRipListenerSetupFailed
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.57

Property name	Value
Default severity	minor
Source stream	main
Message format string	The system could not set up a RIP listener 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.

76.17 sapIfIgnorePortStateStart

Table 1534: 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
Source stream	main
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.

76.18 sapIfIgnorePortStateStop

Table 1535: 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
Source stream	main
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.

76.19 sapIpipeCeIpAddrChange

Table 1536: 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
Source stream	main
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.

Property name	Value
	The IP address type is specified by sapIpipeCeIpAddrType. The IP address is specified by sapIpipeCeIpAddress.
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.

76.20 sapPortStateChangeProcessed

Table 1537: 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
Source stream	main
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

76.21 sapReceivedPbbProtSrcMac

Table 1538: sapReceivedPbbProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2247
Event name	sapReceivedPbbProtSrcMac
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.63
Default severity	minor
Source stream	main
Message format string	MAC *$protectedMacForNotify$* protected in i-vpls *$svcId$* received on SAP *$sapEncapValue$* in b-vpls service *$svcTlsBackboneVplsSvcId$*.
Cause	The sapReceivedPbbProtSrcMac notification is generated when a protected source MAC protected in i-vpls is received on SAP in b-vpls (svcTlsBackboneVplsSvcId) service.
Effect	The frame is discarded.
Recovery	None needed.

76.22 sapReceivedProtSrcMac

Table 1539: sapReceivedProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2208
Event name	sapReceivedProtSrcMac
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.15
Default severity	minor
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	N/A

76.23 sapStatusChanged

Table 1540: 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
Source stream	main
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

76.24 sapTlsDataSapInstStatusChgd

Table 1541: sapTlsDataSapInstStatusChgd properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2532
Event name	sapTlsDataSapInstStatusChgd
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.28
Default severity	minor
Source stream	main
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

76.25 sapTlsMacAddrLimitAlarmCleared

Table 1542: 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
Source stream	main
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

76.26 sapTlsMacAddrLimitAlarmRaised

Table 1543: 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
Source stream	main
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 high watermark."
Effect	N/A
Recovery	N/A

76.27 sapTlsMacMoveExceeded

Table 1544: 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
Source stream	main

Property name	Value
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sapTlsNotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* and will retry in *$sapTlsMacMoveNextUpTime$* seconds (retries left=*$sapTlsMacMoveRateExcdLeft$* admin= *$sapAdminStatus$* oper=*$sapOperStatus$*) - detected on SAP *$sapEncapValue$*
Cause	The TLS svcTlsMacMoveMaxRate has been exceeded for the SAP.
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 administrator.

76.28 sapTlsMacMoveExceedNonBlock

Table 1545: 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
Source stream	main
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sapTlsNotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* - detected on SAP *$sapEncapValue$*
Cause	The sapTlsMacMoveExceedNonBlock notification is generated when the SAP exceeds the TLS svcTlsMacMoveMaxRate when sapTlsLimitMacMove 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(bVpls), the notification will be generated with svcId, custId of I-VPLS and B-VPLS sapId.

Property name	Value
Effect	This notification is informational only.
Recovery	User can adjust the value of svcTlsMacMoveMaxRate to reduce the frequency of this notification.

76.29 sapTunnelEncapIpMtuTooSmall

Table 1546: sapTunnelEncapIpMtuTooSmall properties

Property name	Value
Application name	SVCMGR
Event ID	2243
Event name	sapTunnelEncapIpMtuTooSmall
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.56
Default severity	warning
Source stream	main
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.

76.30 sapTunnelStateChange

Table 1547: 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
Source stream	main
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.

76.31 sdpBandwidthOverbooked

Table 1548: 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

Property name	Value
Source stream	main
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

76.32 sdpBindEthLoopbackStarted

Table 1549: sdpBindEthLoopbackStarted properties

Property name	Value
Application name	SVCMGR
Event ID	2328
Event name	sdpBindEthLoopbackStarted
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.33
Default severity	minor
Source stream	main
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

76.33 sdpBindEthLoopbackStopped

Table 1550: 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
Source stream	main
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

76.34 sdpBindInsufficientBandwidth

Table 1551: 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
Source stream	main
Message format string	The available bandwidth *$sdpAvailableBandwidth$* of SDP cannot satisfy the bandwidth *$sdpBindAdminBandwidth$* required by the SDP Bind *$sdpBindId$*.

Property name	Value
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

76.35 sdpBindIpipeCeIpAddressChange

Table 1552: 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
Source stream	main
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.
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.

76.36 sdpBindPwLocalStatusBitsChanged

Table 1553: 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
Source stream	main
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.

76.37 sdpBindPwPeerFaultAddrChanged

Table 1554: sdpBindPwPeerFaultAddrChanged properties

Property name	Value
Application name	SVCMGR
Event ID	2315
Event name	sdpBindPwPeerFaultAddrChanged
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.16
Default severity	minor
Source stream	main
Message format string	Status of SDP Bind *$sdpBindId$* in service *$svcId$* (customer *$cust Id$*) peer PW status IP address changed to *$sdpBindPwFaultInet Address$*

Property name	Value
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

76.38 sdpBindPwPeerStatusBitsChanged

Table 1555: 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
Source stream	main
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

76.39 sdpBindReceivedPbbProtSrcMac

Table 1556: sdpBindReceivedPbbProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2367
Event name	sdpBindReceivedPbbProtSrcMac
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.37
Default severity	minor
Source stream	main
Message format string	MAC *$protectedMacForNotify$* protected in i-vpls *$svcId$* is received on SDP Bind *$sdpBindId$* in b-vpls service *$svcTlsBackboneVplsSvcId$*.
Cause	The sdpBindReceivedPbbProtSrcMac notification is generated when a source MAC is protected in a i-vpls is received on SDP-BIND of a b-vpls (svcTlsBackboneVplsSvcId) service.
Effect	The frame will be discarded.
Recovery	No action is required.

76.40 sdpBindReceivedProtSrcMac

Table 1557: 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
Source stream	main
Message format string	Protected MAC *$protectedMacForNotify$* received on SDP Bind *$sdpBindId$* in service *$svcId$*.

Property name	Value
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.

76.41 sdpBindSdpStateChangeProcessed

Table 1558: 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
Source stream	main
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.
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

76.42 sdpBindStatusChanged

Table 1559: 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
Source stream	main
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

76.43 sdpBindTlsMacMoveExceeded

Table 1560: sdpBindTlsMacMoveExceeded properties

Property name	Value
Application name	SVCMGR
Event ID	2314
Event name	sdpBindTlsMacMoveExceeded
SNMP notification prefix and OID	TIMETRA-SDP-MIB.sdpTraps.15
Default severity	minor
Source stream	main
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sdpBind NotifyMacAddr$* exceeded *$svcTlsMacMoveMaxRate$* and will retry in *$sdpBindTlsMacMoveNextUpTime$* seconds (retries left=*$sdpBindTls*

Property name	Value
	MacMoveRateExcdLeft$* admin= *$sdpBindAdminStatus$* oper=*$sdp BindOperStatus$*) - detected on SDP Bind *$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 sdpBindTlsMacMoveRate ExcdLeft, the interface will be brought back up automatically in sdp BindTlsMacMoveNextUpTime seconds. If no retries are remaining, the interface must be manually brought back up by an administrator.

76.44 sdpBindTlsMacMoveExceedNonBlock

Table 1561: 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
Source stream	main
Message format string	Mac move rate for service *$svcId$* (customer *$custId$*), MAC *$sdpBind NotifyMacAddr$* 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 Backbone-VPLS(bVpls), the notification will be generated with svcId, custId of I-VPLS and B-VPLS sdpBindId.
Effect	This notification is informational only.

Property name	Value
Recovery	User can adjust the value of svcTlsMacMoveMaxRate to reduce the frequency of this notification."

76.45 sdpControlPwActiveStateChg

Table 1562: 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
Source stream	main
Message format string	Control PW Active status is *$sdpControlPWIsActive$* on SDP:*$sdpId$*
Cause	The sdpControlPwActiveStateChg notification is generated 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.

76.46 sdpEgrIfsNetDomInconsCntChanged

Table 1563: 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
Source stream	main
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

76.47 sdpKeepAliveLateReply

Table 1564: sdpKeepAliveLateReply properties

Property name	Value
Application name	SVCMGR
Event ID	2310
Event name	sdpKeepAliveLateReply
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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

76.48 sdpKeepAliveProbeFailure

Table 1565: sdpKeepAliveProbeFailure properties

Property name	Value
Application name	SVCMGR
Event ID	2309
Event name	sdpKeepAliveProbeFailure
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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

76.49 sdpKeepAliveStarted

Table 1566: sdpKeepAliveStarted properties

Property name	Value
Application name	SVCMGR
Event ID	2307
Event name	sdpKeepAliveStarted
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	SDP *$sdpId$* keepalive has started
Cause	A sdp keep alive was started.
Effect	N/A
Recovery	N/A

76.50 sdpKeepAliveStopped

Table 1567: sdpKeepAliveStopped properties

Property name	Value
Application name	SVCMGR
Event ID	2308
Event name	sdpKeepAliveStopped
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	SDP *$sdpId$* keepalive has stopped
Cause	A sdp keep alive was stopped.
Effect	N/A
Recovery	N/A

76.51 sdpPbbActvPwWithNonActvCtrlPwChg

Table 1568: 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
Source stream	main
Message format string	First/last PW is active/standby/down (*$sdpPbbActvPwWithNonActvCtrlPw$*) on the BEB where control PW is standby/down on SDP: *$sdpId$*

Property name	Value
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 sdpPbbActvPwWith NonActvCtrlPw set to 'false' indicate clearing of sdpPbbActvPwWithNon ActvCtrlPwChg with sdpPbbActvPwWithNonActvCtrlPw set to 'true'."

76.52 sdpStatusChanged

Table 1569: 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
Source stream	main
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

76.53 sdpTlsMacAddrLimitAlarmCleared

Table 1570: 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
Source stream	main
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

76.54 sdpTlsMacAddrLimitAlarmRaised

Table 1571: 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
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	N/A

76.55 svcArpHostOverride

Table 1572: 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
Source stream	main
Message format string	Existing ARP host (ipAddr = *$svcArpHostIpAddr$*, macAddr = *$svcNotifyMacAddress$*) in service *$svcId$* overridden to (ipAddr = *$svcArpHostIpAddr$*, 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.
Effect	The MAC address of the known ARP host has changed.
Recovery	No recovery required.

76.56 svcArpHostPopulateErr

Table 1573: svcArpHostPopulateErr properties

Property name	Value
Application name	SVCMGR
Event ID	2520

Property name	Value
Event name	svcArpHostPopulateErr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.27
Default severity	warning
Source stream	main
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.

76.57 svcBgpEvpnBHDupMacAddrsDetected

Table 1574: svcBgpEvpnBHDupMacAddrsDetected properties

Property name	Value
Application name	SVCMGR
Event ID	2097
Event name	svcBgpEvpnBHDupMacAddrsDetected
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.83
Default severity	minor
Source stream	main
Message format string	VPLS Service *$svcId$* failed to install black hole destination in FDB for EVPN detected duplicate MAC *$tlsFdbMacAddr$*.
Cause	The svcBgpEvpnBHDupMacAddrsDetected notification is generated when the MAC address(es) detected as duplicate, is not installed in the FDB as blackhole.
Effect	At least one MAC address is detected as duplicate.
Recovery	None needed.

76.58 svcBgpEvpnDupMacAddrsCleared

Table 1575: 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
Source stream	main
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.

76.59 svcBgpEvpnDupMacAddrsDetected

Table 1576: 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
Source stream	main

Property name	Value
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.

76.60 svcBgpEvpnTepStateChgd

Table 1577: svcBgpEvpnTepStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2134
Event name	svcBgpEvpnTepStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.119
Default severity	minor
Source stream	main
Message format string	TEP *$svcBgpEvpnTepStateTEPAddress$* in service *$svcId$* instance *$svcBgpEvpnInstance$* has changed oper-status to (*$svcBgpEvpnTepStateOperState$*) and oper-flags (*$svcBgpEvpnTepStateOperFlags$*)
Cause	Any change to the operational status of the evpn TEP due to the processing of incl-mcast L2 attribute generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.61 svcBindSysHiUsageAlarmCleared

Table 1578: svcBindSysHiUsageAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2342
Event name	svcBindSysHiUsageAlarmCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.53
Default severity	minor
Source stream	main
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.

76.62 svcBindSysHiUsageAlarmRaised

Table 1579: 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
Source stream	main
Message format string	The number of VXLAN bindings in the system exceeds 95% of the system VXLAN bindings limit.

Property name	Value
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.

76.63 svcEndPointMacLimitAlarmCleared

Table 1580: 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
Source stream	main
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

76.64 svcEndPointMacLimitAlarmRaised

Table 1581: 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
Source stream	main
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 an endpoint exceeded the high 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

76.65 svcEpipePbbOperStatusChanged

Table 1582: 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
Source stream	main
Message format string	Operational Status of PBB Tunnel with E-pipe service *$svcId$* changed to *$svcEpipePbbOperState$*.

Property name	Value
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

76.66 svcEPMCEPConfigMismatch

Table 1583: svcEPMCEPConfigMismatch properties

Property name	Value
Application name	SVCMGR
Event ID	2522
Event name	svcEPMCEPConfigMismatch
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.29
Default severity	warning
Source stream	main
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

76.67 svcEPMCEPConfigMismatchResolved

Table 1584: svcEPMCEPConfigMismatchResolved properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2523
Event name	svcEPMCEPConfigMismatchResolved
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.30
Default severity	warning
Source stream	main
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

76.68 svcEPMCEPPassiveModeActive

Table 1585: svcEPMCEPPassiveModeActive properties

Property name	Value
Application name	SVCMGR
Event ID	2524
Event name	svcEPMCEPPassiveModeActive
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.31
Default severity	warning
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	N/A

76.69 svcEPMCEPPassiveModePassive

Table 1586: 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
Source stream	main
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

76.70 svcEvpnESVxVTepLclBiasAddFailClr

Table 1587: svcEvpnESVxVTepLclBiasAddFailClr properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2117
Event name	svcEvpnESVxVTepLclBiasAddFailClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.99
Default severity	minor
Source stream	main
Message format string	Local bias is enabled for vxlan for ethernet-segment *$svcNotifEthSeg Name$*
Cause	The trap svcEvpnESVxVTepLclBiasAddFailClr is raised when the number of local bias peers is less than or equal system limit of three and the failure condition is cleared.
Effect	Vxlan local bias is enabled for the ethernet-segment.
Recovery	None needed.";

76.71 svcEvpnESVxVTepLclBiasAddFailSet

Table 1588: svcEvpnESVxVTepLclBiasAddFailSet properties

Property name	Value
Application name	SVCMGR
Event ID	2115
Event name	svcEvpnESVxVTepLclBiasAddFailSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.97
Default severity	minor
Source stream	main
Message format string	Local bias could not be enabled for ethernet-segment *$svcNotifEthSeg Name$*
Cause	The trap svcEvpnESVxVTepLclBiasAddFailSet is raised when the system limit of three local bias peers per ethernet-segment is exceeded while enabling local bias for a VTEP svcNotifInetAddr.
Effect	Vxlan local bias might not work correctly for all services with ethernet-segment peering to the VTEP.

Property name	Value
Recovery	Configuration change may be required.

76.72 svcEvpnEtreeBumLabelSysHiUsgClr

Table 1589: svcEvpnEtreeBumLabelSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2100
Event name	svcEvpnEtreeBumLabelSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.86
Default severity	minor
Source stream	main
Message format string	The number of EVPN Etree Egress BUM labels received from advertising Etree PEs drops below 90% of the system limit
Cause	The svcEvpnEtreeBumLabelSysHiUsgClr notification is generated when the number of EVPN Etree Egress BUM labels received from advertising Etree PEs in the system drops below 90% of the system limit.
Effect	The number of EVPN Etree Egress BUM labels received from advertising Etree PEs drops below 90%.
Recovery	None needed.

76.73 svcEvpnEtreeBumLabelSysHiUsgSet

Table 1590: svcEvpnEtreeBumLabelSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2099

Property name	Value
Event name	svcEvpnEtreeBumLabelSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.85
Default severity	minor
Source stream	main
Message format string	The number of EVPN Etree Egress BUM labels received from advertising Etree PEs exceeds 95% of the system limit
Cause	The svcEvpnEtreeBumLabelSysHiUsgSet notification is generated when the number of EVPN Etree Egress BUM labels received from advertising Etree PEs in the system exceeds 95% of the system limit.
Effect	The number of EVPN Etree Egress BUM labels received from advertising Etree PEs exceeds 95%.
Recovery	None needed.

76.74 svcEvpnMHAutoEsiConflict

Table 1591: svcEvpnMHAutoEsiConflict properties

Property name	Value
Application name	SVCMGR
Event ID	2610
Event name	svcEvpnMHAutoEsiConflict
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.104
Default severity	minor
Source stream	main
Message format string	The Auto Ethernet segment identifier type-1 has been deleted for Ethernet Segment *$tmnxSvcSysEthSegName$* because the new ID *$tmnxSvcSysEthSegEsi$* conflicts with ES *$tmnxSvcSysConflictingEthSegName$*
Cause	The svcEvpnMHAutoEsiConflict notification is generated when the auto-esi type-1 ESI generated from CE LACP PDUs for an ES conflicts with one already associated to another ES.
Effect	The type-1 ESI currently used on the ES is deleted.

Property name	Value
Recovery	None needed.

76.75 svcEvpnMHAutoEsiCreated

Table 1592: svcEvpnMHAutoEsiCreated properties

Property name	Value
Application name	SVCMGR
Event ID	2609
Event name	svcEvpnMHAutoEsiCreated
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.103
Default severity	minor
Source stream	main
Message format string	An Auto Ethernet Segment Identifier type-1 with ID *$tmnxSvcSysEthSegEsi$* has been automatically created for Ethernet Segment *$tmnxSvcSysEthSegName$*
Cause	The svcEvpnMHAutoEsiCreated notification is generated when the auto-esi type-1 is configured and the ESI is automatically detected from the CE LACP PDUs.
Effect	If the ESI is generated, the Ethernet Segment can become function.
Recovery	None needed.

76.76 svcEvpnMHEsEviDFStateChgd

Table 1593: svcEvpnMHEsEviDFStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2094
Event name	svcEvpnMHEsEviDFStateChgd

Property name	Value
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.80
Default severity	minor
Source stream	main
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.

76.77 svcEvpnMHEsIsidDFStateChgd

Table 1594: svcEvpnMHEsIsidDFStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2095
Event name	svcEvpnMHEsIsidDFStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.81
Default severity	minor
Source stream	main
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.

76.78 svcEvpnMHStandbyStatusChg

Table 1595: svcEvpnMHStandbyStatusChg properties

Property name	Value
Application name	SVCMGR
Event ID	2113
Event name	svcEvpnMHStandbyStatusChg
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.92
Default severity	minor
Source stream	main
Message format string	Vxlan Instance *$svcNotifVxlanInstance$* on service *$svcId$* multi-homing standby *$svcNotifEvpnMHStandbyStatus$*
Cause	The svcEvpnMHStandbyStatusChg notification is generated when there is a change in status of EVPN multi-homing standby.
Effect	EVPN multi-homing standby status has changed.
Recovery	None needed.

76.79 svcEvpnMplsESDestTEPStateChgd

Table 1596: svcEvpnMplsESDestTEPStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2133
Event name	svcEvpnMplsESDestTEPStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.118
Default severity	minor
Source stream	main

Property name	Value
Message format string	TEP *$svcEvpnInstMplsESDestTEPAddress$* in service *$svcId$* instance *$svcBgpEvpnInstance$* on *$tmnxSvcSysEthSegEsi$* label *$svcEvpnInstMplsESDestTEPLabel$* has changed oper-status to (*$svcEvpnInstMplsESDestTEPOperStat$*) and oper-flags (*$svcEvpnInstMplsESDestTEPOperFlag$*)
Cause	Any addition of new unicast/multicast destination or any change to the operational status of the unicast and multicast destinations generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.80 svcEvpnMplsMacMoveExceedNonBlock

Table 1597: 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
Source stream	main
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 svcTlsMacMove MaxRate 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.

76.81 svcEvpnMplsMldpESLblHiUsgClr

Table 1598: svcEvpnMplsMldpESLblHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2621
Event name	svcEvpnMplsMldpESLblHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.122
Default severity	minor
Source stream	main
Message format string	The number of MLDP EVPN ES labels programmed is below 90% of the system limit
Cause	The svcEvpnMplsMldpESLblHiUsgClr notification is generated when the number number of MLDP EVPN ES labels programmed is below 90% of the system limit.
Effect	The system has reached 90% of MLDP EVPN ES programmed labels limit.
Recovery	None needed.

76.82 svcEvpnMplsMldpESLblHiUsgSet

Table 1599: svcEvpnMplsMldpESLblHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2620
Event name	svcEvpnMplsMldpESLblHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.121
Default severity	minor

Property name	Value
Source stream	main
Message format string	The number of MLDP EVPN ES labels programmed exceeds 95% of the system limit
Cause	The svcEvpnMplsMldpESLblHiUsgSet notification is generated when the number of MLDP EVPN ES labels programmed exceeds 95% of the system limit.
Effect	The system has reached 95% of MLDP EVPN ES programmed labels limit.
Recovery	None needed.

76.83 svcEvpnMplsTEPEgrBndSvcHiUsgClr

Table 1600: 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
Source stream	main
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.

76.84 svcEvpnMplsTEPEgrBndSvcHiUsgSet

Table 1601: 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
Source stream	main
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.
Effect	The VPLS service has reached 95% of the EVPN MPLS tunnel endpoint-egress multicast bind multicast limit.
Recovery	None needed.

76.85 svcEvpnMplsTEPEgrBndSysHiUsgClr

Table 1602: 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

Property name	Value
Source stream	main
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.

76.86 svcEvpnMplsTEPEgrBndSysHiUsgSet

Table 1603: svcEvpnMplsTEPEgrBndSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2354
Event name	svcEvpnMplsTEPEgrBndSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.64
Default severity	minor
Source stream	main
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.

76.87 svcEvpnMplsTEPEgrLblStateChgd

Table 1604: svcEvpnMplsTEPEgrLblStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2127
Event name	svcEvpnMplsTEPEgrLblStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.113
Default severity	minor
Source stream	main
Message format string	TEP *$svcEvpnMplsTEPEgrLblTEPAddress$* in service *$svcId$* bgp-instance *$svcBgpEvpnInstance$* with label *$svcEvpnMplsTEPEgr LblTEPLabel$* in tunnel *$svcEvpnInstMplsTEPEgrLblTEPTnlId$* has changed oper-status to (*$svcEvpnInstMplsTEPEgrLblOperStat$*) and oper-flags (*$svcEvpnInstMplsTEPEgrLblOperFlag$*)
Cause	Any addition of new unicast/multicast destination or any change to the operational status of the unicast and multicast destinations generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.88 svcEvpnMplsTEPHiUsageCleared

Table 1605: svcEvpnMplsTEPHiUsageCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2353
Event name	svcEvpnMplsTEPHiUsageCleared
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.63

Property name	Value
Default severity	minor
Source stream	main
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.

76.89 svcEvpnMplsTEPHiUsageRaised

Table 1606: 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
Source stream	main
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.

76.90 svcEvpnMplsTEPIpSysHiUsgClr

Table 1607: svcEvpnMplsTEPIpSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2608
Event name	svcEvpnMplsTEPIpSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.102
Default severity	minor
Source stream	main
Message format string	The number of EVPN MPLS tunnel endpoint ip in the system is below 90% of the system limit
Cause	The svcEvpnMplsTEPIpSysHiUsgClr notification is generated when the number of EVPN MPLS tunnel endpoint IP in the system drops below 90% of the system limit.
Effect	90% of the system EVPN MPLS tunnel endpoint IP limit is reached.
Recovery	None needed.

76.91 svcEvpnMplsTEPIpSysHiUsgSet

Table 1608: svcEvpnMplsTEPIpSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2607
Event name	svcEvpnMplsTEPIpSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.101
Default severity	minor
Source stream	main

Property name	Value
Message format string	The number of EVPN MPLS tunnel endpoint ip in the system exceeds 95% of the system limit
Cause	The svcEvpnMplsTEPIpSysHiUsgSet notification is generated when the number of EVPN MPLS tunnel endpoint IP in the system exceeds 95% of the system limit.
Effect	95% of the system EVPN MPLS tunnel endpoint IP limit is reached.
Recovery	None needed.

76.92 svcEvpnRcvdPbbProtSrcMac

Table 1609: svcEvpnRcvdPbbProtSrcMac properties

Property name	Value
Application name	SVCMGR
Event ID	2118
Event name	svcEvpnRcvdPbbProtSrcMac
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.100
Default severity	minor
Source stream	main
Message format string	Mac *$protectedMacForNotify$* protected in i-vpls *$svcId$* received on EVPN in b-vpls service *$svcTlsBackboneVplsSvcId$*.
Cause	The svcEvpnRcvdPbbProtSrcMac notification is generated when a protected source MAC protected in i-vpls is received on EVPN in b-vpls (svcTlsBackboneVplsSvcId) service.
Effect	The frame is discarded.
Recovery	None needed.

76.93 svcEvpnRcvdProtSrcMac

Table 1610: 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
Source stream	main
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.

76.94 svcEvpnVxInstESDstTEPStateChgd

Table 1611: svcEvpnVxInstESDstTEPStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2130
Event name	svcEvpnVxInstESDstTEPStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.115
Default severity	minor
Source stream	main
Message format string	TEP *$svcEvpnVxlanInstESDstTEPAddress$* in service *$svcId $* vxlan-instance *$svcVxlanInstanceId$* with vni *$svcEvpnVxlan InstESDstTEPVni$* on *$tmnxSvcSysEthSegEsi$* has changed oper-status to (*$svcEvpnVxlanInstESDestTEPOpState$*) and oper-flags (*$svcEvpnVxlanInstESDestTEPOpFlag$*)

Property name	Value
Cause	Any addition of new unicast/multicast destination or any change to the operational status of the unicast and multicast destinations generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.95 svcEvpnVxVTepLclBiasAddFailClr

Table 1612: svcEvpnVxVTepLclBiasAddFailClr properties

Property name	Value
Application name	SVCMGR
Event ID	2116
Event name	svcEvpnVxVTepLclBiasAddFailClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.98
Default severity	minor
Source stream	main
Message format string	Local bias is enabled for vxlan far-end *$svcNotifInetAddr$*
Cause	The trap svcEvpnVxVTepLclBiasAddFailClr is sent whenever local bias failure condition for the Vxlan VTEP svcNotifInetAddr, is cleared.
Effect	Vxlan local bias is enabled for the VTEP.
Recovery	None needed.";

76.96 svcEvpnVxVTepLclBiasAddFailSet

Table 1613: svcEvpnVxVTepLclBiasAddFailSet properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2114
Event name	svcEvpnVxVTepLclBiasAddFailSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.96
Default severity	minor
Source stream	main
Message format string	Local bias could not be enabled for vxlan far-end *$svcNotifInetAddr$* due to system limit
Cause	The trap svcEvpnVxVTepLclBiasAddFailSet is sent whenever local bias cannot be enabled for the Vxlan VTEP svcNotifInetAddr, due to system limits.
Effect	Vxlan local bias might not work correctly for all services with ethernet-segment shared with this VTEP.
Recovery	Configuration change may be required.

76.97 svcFdbMimDestTblFullAlrm

Table 1614: 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
Source stream	main
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.

Property name	Value
Recovery	N/A

76.98 svcFdbMimDestTblFullAlrmCleared

Table 1615: 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
Source stream	main
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
Recovery	N/A

76.99 svcIfSubForwardingStatsDisNotify

Table 1616: svcIfSubForwardingStatsDisNotify properties

Property name	Value
Application name	SVCMGR
Event ID	2614
Event name	svcIfSubForwardingStatsDisNotify
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.108

Property name	Value
Default severity	minor
Source stream	main
Message format string	Statistics for subscriber/group-interface %iesIfIndex% disabled: %tmnxFailureDescription%
Cause	The svcIfSubForwardingStatsDisNotify notification is generated when adding the subscriber/group-interface statistics fail due to exceeded scale limits.
Effect	A log entry is generated.
Recovery	If another subscriber/group-interface returns resources then missing subscriber/group-interfaces are enabled in random order.

76.100 svcIfSubForwardingStatsEnNotify

Table 1617: svcIfSubForwardingStatsEnNotify properties

Property name	Value
Application name	SVCMGR
Event ID	2615
Event name	svcIfSubForwardingStatsEnNotify
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.109
Default severity	minor
Source stream	main
Message format string	Statistics for subscriber/group-interface %iesIfIndex% enabled
Cause	The svcIfSubForwardingStatsEnNotify notification is generated when previously disbaled subscriber/group-interface statistics are enabled again due to available resources.
Effect	A log entry is generated.
Recovery	None.

76.101 svcMSPwRetryExpiredNotif

Table 1618: 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
Source stream	main
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."

76.102 svcMSPwRtMisconfig

Table 1619: svcMSPwRtMisconfig properties

Property name	Value
Application name	SVCMGR
Event ID	2541
Event name	svcMSPwRtMisconfig
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.38
Default severity	minor

Property name	Value
Source stream	main
Message format string	Misconfigured multi-segment pseudo-wire SAII=*$svcMSPwPeSaii GlobalId$*:*$svcMSPwPeSaiiPrefix$*: *$svcMSPwPeSaiiAcId$* TAII= *$svcMSPwPeTaiiGlobalId$*:*$svcMSPwPeTaiiPrefix$*:*$svcMSPwPeTaii AcId$*
Cause	The svcMSPwRtMisconfig notification is raised when there is mis-configuration discovered between two signaling 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.

76.103 svcOperGrpOperStatusChanged

Table 1620: 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
Source stream	main
Message format string	Oper-group *$svcOperGrpName$* changed status to *$svcOperGrpOper Status$*
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.

76.104 svcPersistencyProblem

Table 1621: 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
Source stream	main
Message format string	Persistency problem in service *$svcId$*: *$tmnxFailureDescription$*
Cause	A persistency problem occurred.
Effect	N/A
Recovery	N/A

76.105 svcRestoreHostProblem

Table 1622: 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
Source stream	main
Message format string	Problem occurred while processing host persistency record (Addr = *$svcHostAddr$*) - *$tmnxFailureDescription$*

Property name	Value
Cause	N/A
Effect	N/A
Recovery	N/A

76.106 svcRoutedVplsEvpnGWDrStateChgd

Table 1623: svcRoutedVplsEvpnGWDrStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2616
Event name	svcRoutedVplsEvpnGWDrStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.110
Default severity	minor
Source stream	main
Message format string	The state of Evpn Gateway DR changed to *$svcRoutedVplsEvpnGWDrState$* in service *$svcId$*
Cause	Any addition of new evpn-mcast-gw or deletion of existing evpn-mcast-gw configuration leads to change in the state based on DF election algorithm the node chooses, and generates trap.
Effect	When this state is true, indicates this node will forward the outgoing traffic towards the PIM/MVPN network.
Recovery	Any addition of new evpn-mcast-gw or deletion of existing evpn-mcast-gw configuration leads to change in the state based on DF election algorithm the node chooses, and generates trap.

76.107 svcRvplsEvpnMcastDestSysHiUsgClr

Table 1624: svcRvplsEvpnMcastDestSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2626
Event name	svcRvplsEvpnMcastDestSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.126
Default severity	minor
Source stream	main
Message format string	The number of R-VPLS EVPN multicast destinations falls below the limit
Cause	The svcRvplsEvpnMcastDestSysHiUsgClr notification is generated when number of R-VPLS EVPN multicast destinations goes over the limit.
Effect	Number of R-VPLS EVPN multicast destinations goes over the limit.
Recovery	None needed.

76.108 svcRvplsEvpnMcastDestSysHiUsgSet

Table 1625: svcRvplsEvpnMcastDestSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2625
Event name	svcRvplsEvpnMcastDestSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.125
Default severity	minor
Source stream	main
Message format string	The number of R-VPLS EVPN multicast destinations goes over the limit

Property name	Value
Cause	The svcRvplsEvpnMcastDestSysHiUsgSet notification is generated when number of R-VPLS EVPN multicast destinations goes over the limit.
Effect	Number of R-VPLS EVPN multicast destinations goes over the limit.
Recovery	None needed.

76.109 svcSiteMinDnTimerStateChg

Table 1626: 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
Source stream	main
Message format string	Service:*$svcId$* site:*$svcNotifSiteName$* min-down-timer state changed to:*$svcNotifSiteMinDnTimerState$* with timer: *$svcNotifSite MinDnTimer$* secs and timer-remaining:*$svcNotifSiteMinDnTimer Remain$* 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.

76.110 svcSrv6FunctionOutOfResources

Table 1627: svcSrv6FunctionOutOfResources properties

Property name	Value
Application name	SVCMGR
Event ID	2135
Event name	svcSrv6FunctionOutOfResources
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.120
Default severity	minor
Source stream	main
Message format string	Allocation of *$svcNotifSrv6ExhaustedResource$* failed for *$svcType$ $svcId$* srv6-instance *$svcNotifSrv6Instance$ $svcNotifSrv6Locator Type$ $svcNotifSrv6LocatorName$* function *$svcSrv6FunctionType$* value *$svcSrv6FunctionValue$*.
Cause	The svcSrv6FunctionOutOfResources notification is generated when the function or hardware resource allocation fails.
Effect	A log entry is generated.
Recovery	if another entity or local config change returns resources, then it will be automatically allocated.

76.111 svcSrv6InstESDstTEPOperStateChgd

Table 1628: svcSrv6InstESDstTEPOperStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2132
Event name	svcSrv6InstESDstTEPOperStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.117
Default severity	minor
Source stream	main
Message format string	TEP *$svcSrv6InstESDstTEPAddress$* in service *$svcId$* srv6-instance *$svcSrv6Instance$* on *$svcSrv6InstESDstTEPSidAddr$* has changed

Property name	Value
	oper-status to (*$svcSrv6InstESDstTEPOperState$*) and oper-flags (*$svcSrv6InstESDstTEPOperFlag$*)
Cause	Any addition of new unicast/multicast destination or any change to the operational status of the unicast and multicast destinations generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.112 svcSrv6InstTEPSidOperStateChgd

Table 1629: svcSrv6InstTEPSidOperStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2131
Event name	svcSrv6InstTEPSidOperStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.116
Default severity	minor
Source stream	main
Message format string	TEP *$svcSrv6InstTEPAddress$* in service *$svcId$* srv6-instance *$svcSrv6Instance$* on *$svcSrv6InstTEPSidAddr$* has changed oper-status to (*$svcSrv6InstTEPSidOperState$*) and oper-flags (*$svc Srv6InstTEPSidOperFlag$*)
Cause	Any addition of new unicast/multicast destination or any change to the operational status of the unicast and multicast destinations generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.113 svcSrv6TEPEgrBndSvcHiUsgClr

Table 1630: svcSrv6TEPEgrBndSvcHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2618
Event name	svcSrv6TEPEgrBndSvcHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.112
Default severity	minor
Source stream	main
Message format string	Service *$svcId$* has SRv6 tunnel endpoint-egress multicast binds below 90% of the per-service limit
Cause	The svcSrv6TEPEgrBndSvcHiUsgClr notification is generated when the number of SRv6 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 SRv6 tunnel endpoint-egress multicast bind multicast limit.
Recovery	None needed.

76.114 svcSrv6TEPEgrBndSvcHiUsgSet

Table 1631: svcSrv6TEPEgrBndSvcHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2617
Event name	svcSrv6TEPEgrBndSvcHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.111
Default severity	minor
Source stream	main
Message format string	Service *$svcId$* has SRv6 tunnel endpoint-egress multicast binds in excess of 95% of the per-service limit

Property name	Value
Cause	The svcSrv6TEPEgrBndSvcHiUsgSet notification is generated when the number of SRv6 tunnel endpoint-egress multicast binds in a VPLS service exceeds 95% of the per-service limit.
Effect	The VPLS service has reached 95% of the SRv6 tunnel endpoint-egress multicast bind multicast limit.
Recovery	None needed.

76.115 svcSrv6TEPEgrBndSysHiUsgClr

Table 1632: svcSrv6TEPEgrBndSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2612
Event name	svcSrv6TEPEgrBndSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.106
Default severity	minor
Source stream	main
Message format string	The number of EVPN SRv6 tunnel endpoint-egress binds in the system is below 90% of the system limit
Cause	The svcSrv6TEPEgrBndSysHiUsgClr notification is generated when the number of EVPN SRv6 tunnel endpoint-egress binds in the system drops below 90% of the system limit.
Effect	90% of the system EVPN SRv6 tunnel endpoint-egress bind limit is reached.
Recovery	None needed.

76.116 svcSrv6TEPEgrBndSysHiUsgSet

Table 1633: svcSrv6TEPEgrBndSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2611
Event name	svcSrv6TEPEgrBndSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.105
Default severity	minor
Source stream	main
Message format string	The number of EVPN SRv6 tunnel endpoint-egress binds in the system exceeds 95% of the system limit
Cause	The svcSrv6TEPEgrBndSysHiUsgSet notification is generated when the number of EVPN SRv6 tunnel endpoint-egress multicast binds in the system exceeds 95% of the system limit.
Effect	95% of the system EVPN SRv6 tunnel endpoint-egress multicast bind limit is reached.
Recovery	None needed.

76.117 svcStatusChanged

Table 1634: 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
Source stream	main
Message format string	Status of service *$svcId$* (customer *$custId$*) changed to administrative state: *$svcAdminStatus$*, operational state: *$svcOper Status$*

Property name	Value
Cause	There was a change in the administrative or operating status of a service.
Effect	N/A
Recovery	N/A

76.118 svcSysEvpnESDfPrefOperValChange

Table 1635: 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
Source stream	main
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.

76.119 svcTlsEvpnTunnNHopHiUsgAlarmClr

Table 1636: svcTlsEvpnTunnNHopHiUsgAlarmClr properties

Property name	Value
Application name	SVCMGR
Event ID	2351
Event name	svcTlsEvpnTunnNHopHiUsgAlarmClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.61
Default severity	minor
Source stream	main
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.

76.120 svcTlsEvpnTunnNHopHiUsgAlarmSet

Table 1637: 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
Source stream	main
Message format string	Reached 95% of EVPN tunnel interface IP next-hop limit for service *$svcId$*

Property name	Value
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."

76.121 svcTlsFdbTableFullAlarmCleared

Table 1638: 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
Source stream	main
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

76.122 svcTlsFdbTableFullAlarmRaised

Table 1639: 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
Source stream	main
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

76.123 svcTlsGroupOperStatusChanged

Table 1640: 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
Source stream	main
Message format string	Service *$svcId$* VPLS group *$svcTlsGroupId$* changed status to *$svc TlsGroupOperStatus$* with last-error: *$svcTlsGroupLastError$*
Cause	Service VPLS Group status changed
Effect	N/A

Property name	Value
Recovery	N/A

76.124 svcTlsMacPinningViolation

Table 1641: 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
Source stream	main
Message format string	Relearn attempt on *$macPinningViolatingRowDescr$* in service *$svcId $* for mac address *$macPinningMacAddress$* pinned on *$macPinning PinnedRowDescr$*
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
Recovery	No recovery is necessary.

76.125 svcTlsMfibTableFullAlarmCleared

Table 1642: svcTlsMfibTableFullAlarmCleared properties

Property name	Value
Application name	SVCMGR
Event ID	2402
Event name	svcTlsMfibTableFullAlarmCleared

Property name	Value
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.10
Default severity	minor
Source stream	main
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

76.126 svcTlsMfibTableFullAlarmRaised

Table 1643: 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
Source stream	main
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.
Effect	N/A
Recovery	N/A

76.127 svcTlsMrpAttrRegistrationFailed

Table 1644: 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
Source stream	main
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

76.128 svcTlsMrpAttrTblFullAlarmCleared

Table 1645: 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
Source stream	main
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

Property name	Value
Recovery	N/A

76.129 svcTlsMrpAttrTblFullAlarmRaised

Table 1646: 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
Source stream	main
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

76.130 svcTlsProxyArpDupClear

Table 1647: svcTlsProxyArpDupClear properties

Property name	Value
Application name	SVCMGR
Event ID	2347
Event name	svcTlsProxyArpDupClear
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.57

Property name	Value
Default severity	minor
Source stream	main
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.

76.131 svcTlsProxyArpDupDetect

Table 1648: 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
Source stream	main
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."

76.132 svcTlsProxyArpSvcHiUsgClr

Table 1649: 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
Source stream	main
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.

76.133 svcTlsProxyArpSvcHiUsgSet

Table 1650: 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
Source stream	main

Property name	Value
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.
Recovery	None needed.

76.134 svcTlsProxyArpSysHiUsgClr

Table 1651: 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
Source stream	main
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.

76.135 svcTlsProxyArpSysHiUsgSet

Table 1652: 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
Source stream	main
Message format string	The proxy ARP entries in the system exceeds 95% of the system limit
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.

76.136 svcTlsProxyArpUnauthorizedIP

Table 1653: svcTlsProxyArpUnauthorizedIP properties

Property name	Value
Application name	SVCMGR
Event ID	2622
Event name	svcTlsProxyArpUnauthorizedIP
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.123
Default severity	minor
Source stream	main
Message format string	An attempt to create an unauthorized proxy-arp entry was made for entry IP *$svcTlsProxyArpIpAddr$* in service *$svcId$*
Cause	The svcTlsProxyArpUnauthorizedIP notification is generated when an attempt to create a unauthorized proxy ARP entry IP was made.

Property name	Value
Effect	Restrict unauthorized ARP requests.
Recovery	None needed.

76.137 svcTlsProxyNdDupClear

Table 1654: 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
Source stream	main
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.

76.138 svcTlsProxyNdDupDetect

Table 1655: svcTlsProxyNdDupDetect properties

Property name	Value
Application name	SVCMGR
Event ID	2348
Event name	svcTlsProxyNdDupDetect

Property name	Value
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.58
Default severity	minor
Source stream	main
Message format string	A duplicate proxy ND entry was detected with new MAC *$svcNotifTlsProxyMacAddr$* for entry IP *$svcTlsProxyArpIpAddr$* MAC *$svcTlsProxyArpMacAddr$* 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."

76.139 svcTlsProxyNdSvcHiUsgClr

Table 1656: 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
Source stream	main
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.

76.140 svcTlsProxyNdSvcHiUsgSet

Table 1657: 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
Source stream	main
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.

76.141 svcTlsProxyNdSysHiUsgClr

Table 1658: 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
Source stream	main

Property name	Value
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.

76.142 svcTlsProxyNdSysHiUsgSet

Table 1659: 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
Source stream	main
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.

76.143 svcTlsProxyNdUnauthorizedIP

Table 1660: svcTlsProxyNdUnauthorizedIP properties

Property name	Value
Application name	SVCMGR
Event ID	2623
Event name	svcTlsProxyNdUnauthorizedIP
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.124
Default severity	minor
Source stream	main
Message format string	An attempt to create an unauthorized proxy-nd entry was made for entry IP *$svcTlsProxyArpIpAddr$* in service *$svcId$*
Cause	The svcTlsProxyNdUnauthorizedIP notification is generated when an attempt to create a unauthorized proxy ND entry IP was made.
Effect	Restrict unauthorized neighbor recovery requests.
Recovery	None needed.

76.144 svcTlsSiteDesigFwdrChg

Table 1661: 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
Source stream	main
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.

Property name	Value
Effect	N/A
Recovery	N/A

76.145 svcTlsVTEPEgrVniSvcHiUsgAlarmClr

Table 1662: 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
Source stream	main
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.

76.146 svcTlsVTEPEgrVniSvcHiUsgAlarmSet

Table 1663: svcTlsVTEPEgrVniSvcHiUsgAlarmSet properties

Property name	Value
Application name	SVCMGR
Event ID	2339

Property name	Value
Event name	svcTlsVTEPEgrVniSvcHiUsgAlarmSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.50
Default severity	minor
Source stream	main
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.

76.147 svcTlsVTEPEgrVniSysHiUsgAlarmClr

Table 1664: 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
Source stream	main
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.

76.148 svcTlsVTEPEgrVniSysHiUsgAlarmSet

Table 1665: svcTlsVTEPEgrVniSysHiUsgAlarmSet properties

Property name	Value
Application name	SVCMGR
Event ID	2337
Event name	svcTlsVTEPEgrVniSysHiUsgAlarmSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.48
Default severity	minor
Source stream	main
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.

76.149 svcTlsVTEPHiUsageAlarmCleared

Table 1666: 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
Source stream	main

Property name	Value
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.

76.150 svcTlsVTEPHiUsageAlarmRaised

Table 1667: 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
Source stream	main
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.

76.151 svcTlsVxInstMacAdrLimitAlrmClrd

Table 1668: svcTlsVxInstMacAdrLimitAlrmClrd properties

Property name	Value
Application name	SVCMGR
Event ID	2601
Event name	svcTlsVxInstMacAdrLimitAlrmClrd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.95
Default severity	minor
Source stream	main
Message format string	Mac address limit for service *$svcId$*, vpn *$svcVpnId$*, vxlan instance *$svcVxlanInstanceId$* dropped below the low watermark
Cause	The trap svcTlsVxInstMacAdrLimitAlrmClrd is sent whenever the number of MAC addresses stored in the FDB for this VXLAN instance, drops to the watermark specified by the object svcTlsFdbTableFullLow Watermark.
Effect	The number of MAC addresses stored in the FDB drops below svcTls FdbTableFullLowWatermark.
Recovery	None needed.

76.152 svcTlsVxInstMacAdrLimitAlrmRsd

Table 1669: svcTlsVxInstMacAdrLimitAlrmRsd properties

Property name	Value
Application name	SVCMGR
Event ID	2600
Event name	svcTlsVxInstMacAdrLimitAlrmRsd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.94
Default severity	minor
Source stream	main
Message format string	Mac address limit for service *$svcId$*, vpn *$svcVpnId$*, vxlan instance *$svcVxlanInstanceId$* reached the high watermark

Property name	Value
Cause	The trap svcTlsVxInstMacAdrLimitAlrmRsd is sent whenever the number of MAC addresses stored in the FDB for this VXLAN instance, increases to reach the watermark specified by the object svcTlsFdb TableFullHighWatermark.
Effect	The number of MAC addresses stored in the FDB, increases to reach the watermark specified by svcTlsFdbTableFullHighWatermark.
Recovery	None needed.

76.153 svcTlsVxInstReplicatorChgd

Table 1670: svcTlsVxInstReplicatorChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2090
Event name	svcTlsVxInstReplicatorChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.93
Default severity	minor
Source stream	main
Message format string	Assisted replicator in service *$svcId$* changed to VTEP *$svcTls VxInstVTEPAddress$*, Egress VNI *$svcTlsVxInstVTEPEgrVni$* vxlan-instance *$svcNotifVxlanInstance$*.
Cause	The svcTlsVxInstReplicatorChgd notification is generated when there is a change in the replicator.
Effect	The replicator associated with a VPLS service is changed.
Recovery	None needed.

76.154 svcTlsVxInstVTEPEgrVniStateChgd

Table 1671: svcTlsVxInstVTEPEgrVniStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2129
Event name	svcTlsVxInstVTEPEgrVniStateChgd
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.114
Default severity	minor
Source stream	main
Message format string	TEP *$svcTlsVxInstVTEPAddress$* in service *$svcId$* vxlan-instance *$svcVxlanInstanceId$* with vni *$svcTlsVxInstVTEPEgrVni$* has changed oper-status to (*$svcTlsVxInstVTEPEgrVniOperState$*) and oper-flags (*$svcTlsVxInstVTEPEgrVniOperFlag$*)
Cause	Any addition of new unicast/multicast destination or any change to the operational status of the unicast and multicast destinations generates the trap.
Effect	A log entry that the operational status has changed is generated.
Recovery	None needed.

76.155 svcVllSiteDesigFwdrChg

Table 1672: 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
Source stream	main
Message format string	Service-id *$svcId$* site *$svcVllSiteIdName$* is *$svcVllSiteIdDesignated Fwdr$* the designated-forwarder

Property name	Value
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.

76.156 svcVxlanEvpnMplsDestSysHiUsgClr

Table 1673: svcVxlanEvpnMplsDestSysHiUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2102
Event name	svcVxlanEvpnMplsDestSysHiUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.88
Default severity	minor
Source stream	main
Message format string	The number of EVPN destinations (MPLS and VXLAN) in the system is below 90% of the system limit
Cause	The svcVxlanEvpnMplsDestSysHiUsgClr 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.

76.157 svcVxlanEvpnMplsDestSysHiUsgSet

Table 1674: svcVxlanEvpnMplsDestSysHiUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2101
Event name	svcVxlanEvpnMplsDestSysHiUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.87
Default severity	minor
Source stream	main
Message format string	The number of EVPN destinations(MPLS and VXLAN) in the system exceeds 95% of the system limit
Cause	The svcVxlanEvpnMplsDestSysHiUsgSet notification is generated when the number of EVPN destinations(MPLS and VXLAN) in the system exceeds 95% of the system limit.
Effect	95% of the system EVPN destinations(MPLS and VXLAN) limit is reached.
Recovery	None needed.

76.158 tmnxEndPointTxActiveChanged

Table 1675: 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
Source stream	main
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

76.159 tmnxIpTunnelOperRemIpChg

Table 1676: 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
Source stream	main
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.

76.160 tmnxIpTunnelOperStateChange

Table 1677: tmnxIpTunnelOperStateChange properties

Property name	Value
Application name	SVCMGR
Event ID	2244
Event name	tmnxIpTunnelOperStateChange
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.59
Default severity	minor
Source stream	main
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

76.161 tmnxPfcpAssocPathMgmtStateChgd

Table 1678: tmnxPfcpAssocPathMgmtStateChgd properties

Property name	Value
Application name	SVCMGR
Event ID	2604
Event name	tmnxPfcpAssocPathMgmtStateChgd
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.53
Default severity	warning
Source stream	main

Property name	Value
Message format string	PFCP association *$tmnxPfcpAssocName$* path management state changed to *$tmnxPfcpAssocPathMgmtState$* - *$tmnxPfcpAssoc RestartReason$*
Cause	The path management state is monitored using heartbeat messages. The path management state may change when the system starts/stops sending heartbeat messages to a peer, or when it starts/stops receiving replies to heartbeat messages.
Effect	Only while the path management state is 'up', new CUPS subscriber sessions can be set up.
Recovery	The recovery action, if any, depends on the root cause of the failure.

76.162 tmnxSapMRtCpeChkStatusChange

Table 1679: tmnxSapMRtCpeChkStatusChange properties

Property name	Value
Application name	SVCMGR
Event ID	2619
Event name	tmnxSapMRtCpeChkStatusChange
SNMP notification prefix and OID	TIMETRA-SAP-MIB.sapTraps.64
Default severity	warning
Source stream	main
Message format string	The managed route *$tmnxSapMRtCpeChkMRtAddr$*/*$tmnxSapMRt CpeChkMRtPrefixLen$* is now *$tmnxSapMRtCpeChkStatus$* (service= *$svcId$* sap=*$sapEncapValue$* host-ip=*$tmnxSapMRtCpeChkHost Addr$* host-mac=*$tmnxSapMRtCpeChkHostMacAddress$*)
Cause	The CPE with address tmnxSapMRtCpeChkAddr becomes unreachable or reachable again according to the conditions specified in the tmnxSapMRtCpeChkEntry and while the value of tmnxSapMRtCpe ChkEnableLog is equal to 'true'.
Effect	The system can not forward traffic to the CPE while it is unreachable; the CPE may be reachable via another system. While the CPE is unreachable, the system can change the operational metric or preference of the associated managed route, according to the tmnx SapMRtCpeChkEntry configuration.

Property name	Value
Recovery	Depending on the situation. If the CPE is reachable via another system, no recovery may be necessary.

76.163 tmnxSapStpExcepCondStateChng

Table 1680: 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
Source stream	main
Message format string	The stp exception condition state for service *$svcId$* (customer *$custId $*) on SAP *$sapEncapValue$* has changed to *$sapTlsStpException$*
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

76.164 tmnxStpRootGuardViolation

Table 1681: tmnxStpRootGuardViolation properties

Property name	Value
Application name	SVCMGR
Event ID	2043
Event name	tmnxStpRootGuardViolation

Property name	Value
SNMP notification prefix and OID	TIMETRA-SAP-MIB.tstpTraps.35
Default severity	minor
Source stream	main
Message format string	A root-guard violation is detected for service *$svcId$* on SAP *$sapEncapValue$*
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

76.165 tmnxSubAcctPlcyFailure

Table 1682: 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
Source stream	main
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

76.166 tmnxSubAcctPlcyRadSerOperStatChg

Table 1683: 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
Source stream	main
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.

76.167 tmnxSubAuthPlcyRadSerOperStatChg

Table 1684: 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

Property name	Value
Source stream	main
Message format string	Subscriber Authentication RADIUS server *$tmnxSubAuthPlcyRadServ Address$* operational status changed to *$tmnxSubAuthPlcyRadServ OperState$*.
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.

76.168 tmnxSubBrgCreated

Table 1685: 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
Source stream	main
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.

76.169 tmnxSubBrgCvlnitFailed

Table 1686: tmnxSubBrgCvInitFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2566
Event name	tmnxSubBrgCvInitFailed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.40
Default severity	warning
Source stream	main
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.

76.170 tmnxSubBrgDeleted

Table 1687: 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
Source stream	main

Property name	Value
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.

76.171 tmnxSubBrgRadiusAuthError

Table 1688: 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
Source stream	main
Message format string	Could not authenticate the Bridged Residential Gateway *$tmnxSubBrg Id$ - $tmnxSubRadiusSubAuthReason$*
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.

76.172 tmnxSubBrgRadiusCoaError

Table 1689: 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
Source stream	main
Message format string	Could not apply a Radius update for the Bridged Residential Gateway *$tmnxSubBrgId$ - $tmnxSubRadiusCoAReason$*
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.

76.173 tmnxSubBrgRadiusProxyAuthError

Table 1690: tmnxSubBrgRadiusProxyAuthError properties

Property name	Value
Application name	SVCMGR
Event ID	2574
Event name	tmnxSubBrgRadiusProxyAuthError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.47
Default severity	warning
Source stream	main

Property name	Value
Message format string	Could not proxy-authenticate the Bridged Residential Gateway *$tmnx SubBrgId$ - $tmnxSubRadiusSubAuthReason$*
Cause	The tmnxSubBrgRadiusProxyAuthError notification indicates that the system encountered a problem while trying to authenticate a Bridged Residential Gateway (BRG) through a radius proxy.
Effect	No hosts associated with the BRG are reachable via this system.
Recovery	Depends on the details of the failure.

76.174 tmnxSubBrgRadiusUpdateIpoeSeFail

Table 1691: 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
Source stream	main
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 occurs 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.

76.175 tmnxSubBrgSessionLimitReached

Table 1692: 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
Source stream	main
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 cannot set up the IPoE session.
Recovery	Not required. This notification is informational.

76.176 tmnxSubCupsUpIfCreationFailed

Table 1693: tmnxSubCupsUpIfCreationFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2603
Event name	tmnxSubCupsUpIfCreationFailed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.52
Default severity	minor

Property name	Value
Source stream	main
Message format string	Could not create *$iesIfType$* interface *$iesIfName$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	A failure occurs while the CUPS User Plane tries to create an interface. The object tmnxSubAdditionalInfo provides more information about the failure.
Effect	The interface is not created. It is impossible to create the SAPs that would be associated with it. Subscriber sessions that need these SAPs cannot become operational.
Recovery	The recovery action depends on the root cause of the failure.

76.177 tmnxSubCupsUpSapCreationFailed

Table 1694: tmnxSubCupsUpSapCreationFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2602
Event name	tmnxSubCupsUpSapCreationFailed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.51
Default severity	minor
Source stream	main
Message format string	Could not create SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	A failure occurs while the CUPS User Plane tries to create a SAP. The object tmnxSubAdditionalInfo provides more information about the failure.
Effect	The SAP is not created. The associated subscriber session cannot become operational.
Recovery	The recovery action depends on the root cause of the failure.

76.178 tmnxSubDhcpOverloadDetected

Table 1695: tmnxSubDhcpOverloadDetected properties

Property name	Value
Application name	SVCMGR
Event ID	2572
Event name	tmnxSubDhcpOverloadDetected
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.46
Default severity	warning
Source stream	main
Message format string	DHCP message processing overload detected: *$tmnxSubSysChassDhcpOverload$*
Cause	The system issues the tmnxSubDhcpOverloadDetected notification when its subscriber management function drops too many DHCP packets, and when the situation returns to normal again. A typical root cause is a too short DHCP lease time.
Effect	The indication should come well before there is noticeable effect on subscriber service.
Recovery	A typical recovery action would be to configure a longer DHCP lease time.

76.179 tmnxSubHostInconsistentAtmTdOvr

Table 1696: 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

Property name	Value
Default severity	warning
Source stream	main
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."
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."

76.180 tmnxSubHostInfoConflict

Table 1697: 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
Source stream	main
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.

76.181 tmnxSubHostLcktLimitReached

Table 1698: 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
Source stream	main
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	N/A
Recovery	N/A

76.182 tmnxSubHostLcktSapLimitReached

Table 1699: 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
Source stream	main

Property name	Value
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	N/A
Recovery	N/A

76.183 tmnxSubInfoEgrAggRateLimitLowReq

Table 1700: tmnxSubInfoEgrAggRateLimitLowReq properties

Property name	Value
Application name	SVCMGR
Event ID	2605
Event name	tmnxSubInfoEgrAggRateLimitLowReq
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.54
Default severity	warning
Source stream	main
Message format string	Subscriber *$tmnxSubInfoSubIdent$*: attempt to limit egress aggregate rate below reserved minimum (*$tmnxSubAdditionalInfo$*) - *$tmnxSubInfoEgrAggRateLimitLow$*
Cause	The system has received a request to reduce the egress aggregate rate below the minimum reserved bandwidth (and it has set the egress aggregate rate to the minimum reserved bandwidth). Such a request may come from Radius or IGMP, for example.
Effect	The subscriber can use less than the bandwidth requested (for multicast traffic, typically), but maintains the minimum reserved bandwidth (for high priority unicast traffic, typically).
Recovery	The recovery action, if any is needed, depends on the root cause.

76.184 tmnxSubIpoeInvalidCidRidChange

Table 1701: tmnxSubIpoeInvalidCidRidChange properties

Property name	Value
Application name	SVCMGR
Event ID	2555
Event name	tmnxSubIpoeInvalidCidRidChange
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.29
Default severity	warning
Source stream	main
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 cannot setup the IPoE session.
Recovery	No recovery is required on this system.

76.185 tmnxSubIpoeInvalidSessionKey

Table 1702: 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
Source stream	main

Property name	Value
Message format string	IPoE session key failure for host with MAC address *$tmnxSubNotif MacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSub AdditionalInfo$*
Cause	The IPoE session key is invalid.
Effect	The system cannot setup the IPoE session.
Recovery	No recovery is required on this system.

76.186 tmnxSubIpoeMigrHostDeleted

Table 1703: tmnxSubIpoeMigrHostDeleted properties

Property name	Value
Application name	SVCMGR
Event ID	2559
Event name	tmnxSubIpoeMigrHostDeleted
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.33
Default severity	warning
Source stream	main
Message format string	IPoE session migration deleted host *$tmnxSubNotifIpAddr$*/ *$tmnx SubNotifPrefixLength$* 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.

76.187 tmnxSubIpoePersistenceRecovery

Table 1704: tmnxSubIpoePersistenceRecovery properties

Property name	Value
Application name	SVCMGR
Event ID	2557
Event name	tmnxSubIpoePersistenceRecovery
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.31
Default severity	warning
Source stream	main
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 cannot setup the IPoE session.
Recovery	No recovery is required on this system.

76.188 tmnxSubIpoeSessionBrgNotAuth

Table 1705: tmnxSubIpoeSessionBrgNotAuth properties

Property name	Value
Application name	SVCMGR
Event ID	2575
Event name	tmnxSubIpoeSessionBrgNotAuth
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.48
Default severity	warning
Source stream	main
Message format string	IPoE session BRG not authenticated failure for host of BRG *$tmnx SubBrgId$* with MAC address *$tmnxSubNotifMacAddr$* on SAP *$sap EncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*

Property name	Value
Cause	The IPoE session is associated with a BRG that is not yet authenticated.
Effect	The system cannot setup the IPoE session.
Recovery	No recovery is required on this system.

76.189 tmnxSubIpoeSessionLimitReached

Table 1706: tmnxSubIpoeSessionLimitReached properties

Property name	Value
Application name	SVCMGR
Event ID	2556
Event name	tmnxSubIpoeSessionLimitReached
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.30
Default severity	warning
Source stream	main
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 cannot setup the IPoE session.
Recovery	No recovery is required on this system.

76.190 tmnxSubIpoeWppRegistrationFailed

Table 1707: tmnxSubIpoeWppRegistrationFailed properties

Property name	Value
Application name	SVCMGR

Property name	Value
Event ID	2606
Event name	tmnxSubIpoeWppRegistrationFailed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.55
Default severity	warning
Source stream	main
Message format string	IPoE session registration failure for host with MAC address *$tmnxSubNotifMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* - *$tmnxSubAdditionalInfo$*
Cause	The cause is given in tmnxSubAdditionalInfo.
Effect	The system cannot setup the IPoE session.
Recovery	No recovery is required on this system.

76.191 tmnxSubMcsRelatedProblem

Table 1708: 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
Source stream	main
Message format string	Problem encountered in Subscriber Management, while performing Multi Chassis Syncing: *$tmnxSubMcsRelatedProblemDescr$*
Cause	A subscriber management specific problem occurred during Multi Chassis Syncing, e.g. of DHCP lease states. The problem is described in the object tmnxSubMcsRelatedProblemDescr.
Effect	N/A
Recovery	N/A

76.192 tmnxSubMngdHostCreationFail

Table 1709: 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
Source stream	main
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.

76.193 tmnxSubMngdHostOverride

Table 1710: 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

Property name	Value
Default severity	warning
Source stream	main
Message format string	Existing managed host IP *$tmnxSubMngdHostIpAddr$* MAC *$tmnx SubMngdHostMacAddr$* on SAP *$sapEncapValue$* in service *$svcId$* overridden - *$tmnxSubAdditionalInfo$*
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.

76.194 tmnxSubPlBndFailed

Table 1711: 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
Source stream	main
Message format string	Could not create an IP address binding in home-aware pool *$tmnxSub NotifName$* 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.

76.195 tmnxSubPysrosExec

Table 1712: tmnxSubPysrosExec properties

Property name	Value
Application name	SVCMGR
Event ID	2627
Event name	tmnxSubPysrosExec
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.59
Default severity	warning
Source stream	main
Message format string	Run #*$smRunIndex$* of script-policy "*$smLaunchName$*" created by owner " *$smLaunchOwner$*" invoked. Triggered by subscriber *$tmnxSubIdent$* [svc: *$svcName$*, sap: *$sapEncapValue$*, mac: *$tmnxSubNotifMacAddr$*, sid: *$tmnxSubNotifPppoeSessionId$* circuit-id: *$tmnxSubNotifCircuitId$* remote-id: *$tmnxSubNotifRemoteId$*]
Cause	The system is triggered by Radius to execute a pySROS script.
Effect	The system attempts to execute the pySROS script.
Recovery	Not applicable.

76.196 tmnxSubPysrosExecFail

Table 1713: tmnxSubPysrosExecFail properties

Property name	Value
Application name	SVCMGR
Event ID	2628
Event name	tmnxSubPysrosExecFail
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.60
Default severity	warning

Property name	Value
Source stream	main
Message format string	Failed to invoke script-policy "*$smLaunchName$*" created by owner " *$smLaunchOwner$*": *$tmnxSubAdditionalInfo$*. Triggered by subscriber *$tmnxSubIdent$* [svc: *$svcName$*, sap: *$sapEncapValue$*, mac: *$tmnxSubNotifMacAddr$*, sid: *$tmnxSubNotifPppoeSessionId$* circuit-id: *$tmnxSubNotifCircuitId$* remote-id: *$tmnxSubNotifRemoteId$*]
Cause	The system encountered a runtime failure while executing a pySROS script.
Effect	The effect depends on the contents of the script.
Recovery	Recovery depends on the contents of the script and on the failure cause.

76.197 tmnxSubRadiusCoaNatFwdFailed

Table 1714: tmnxSubRadiusCoaNatFwdFailed properties

Property name	Value
Application name	SVCMGR
Event ID	2576
Event name	tmnxSubRadiusCoaNatFwdFailed
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.49
Default severity	warning
Source stream	main
Message format string	After a Radius update, failed to create NAT port forwarding entry: subscriber " *$tmnxSubIdent$*" (*$tmnxSubNotifIpAddr$*) protocol *$tmnxSubNotifIpProtocol$* port *$tmnxSubNotifIpPort$* policy " *$tmnxSubNotifName$*" - *$tmnxSubAdditionalInfo$*
Cause	The tmnxSubRadiusCoaNatFwdFailed notification indicates that the system, while processing a Radius Change of Authorization (CoA) request for a Bridged Residential Gateway (BRG) or a subscriber, could not create the requested NAT (or firewall) port forwarding entry. The object tmnxSubNotifIpAddr indicates the inside IP address, and the object tmnxSubNotifName the name of the NAT policy or the firewall policy of the requested NAT port forwarding entry.

Property name	Value
Effect	The BRG or subscriber does not have the requested NAT port forwarding entry.
Recovery	Depends on the details of the failure.

76.198 tmnxSubRadSapCoAError

Table 1715: tmnxSubRadSapCoAError properties

Property name	Value
Application name	SVCMGR
Event ID	2511
Event name	tmnxSubRadSapCoAError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.10
Default severity	warning
Source stream	main
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) request from a Radius server.
Effect	N/A
Recovery	N/A

76.199 tmnxSubRadSapDisconnectError

Table 1716: tmnxSubRadSapDisconnectError properties

Property name	Value
Application name	SVCMGR
Event ID	2509

Property name	Value
Event name	tmnxSubRadSapDisconnectError
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.8
Default severity	warning
Source stream	main
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

76.200 tmnxSubRadSapSubAuthError

Table 1717: 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
Source stream	main
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

76.201 tmnxSubRadSdpBndCoAError

Table 1718: 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
Source stream	main
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
Recovery	No recovery is necessary.

76.202 tmnxSubRadSdpBndDisconnectError

Table 1719: 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
Source stream	main

Property name	Value
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

76.203 tmnxSubRadSdpBndSubAuthError

Table 1720: 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
Source stream	main
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.

76.204 tmnxSubscriberCreated

Table 1721: 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
Source stream	main
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.

76.205 tmnxSubscriberDeleted

Table 1722: tmnxSubscriberDeleted properties

Property name	Value
Application name	SVCMGR
Event ID	2501
Event name	tmnxSubscriberDeleted
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.2
Default severity	warning
Source stream	main
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.

76.206 tmnxSubscriberRenamed

Table 1723: 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
Source stream	main
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.

76.207 tmnxSubSlaacOverride

Table 1724: tmnxSubSlaacOverride properties

Property name	Value
Application name	SVCMGR
Event ID	2022
Event name	tmnxSubSlaacOverride
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.25
Default severity	warning
Source stream	main
Message format string	Existing SLAAC host (*$tmnxSubSlaacPfx$*/*$tmnxSubSlaacPfxLen$*, *$tmnxSubSlaacMacAddr$*) on SAP *$tmnxSubSlaacEncapValue$* in

Property name	Value
	service *$svcId$* overridden by DHCP6 lease-state (*$svcDhcpLease CiAddr$*/*$svcDhcpLeaseCiAddrMaskLen$*, *$svcDhcpLeaseNextHop MacAddr$*)
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

76.208 tmnxSubSlaacSetupFailure

Table 1725: 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
Source stream	main
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."

76.209 tmnxSubStatsResourceLimitReached

Table 1726: tmnxSubStatsResourceLimitReached properties

Property name	Value
Application name	SVCMGR
Event ID	2571
Event name	tmnxSubStatsResourceLimitReached
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.45
Default severity	warning
Source stream	main
Message format string	The system has *$tmnxSubSysChassStatsUsed$* subscribers with accumulated statistics and is above/below its limit of *$tmnxSubNotif Number$*
Cause	The system issues the tmnxSubStatsResourceLimitReached notification when it fails to allocate resources to maintain accumulated statistics for a subscriber, because its limit to the number of subscribers allowed to have such statistics is exceeded. The accumulated statistics are accessible through the tmnxSubStatsEgrPTable, tmnxSubStats EgrQTable and tmnxSubStatsIngTable. The limit may depend on the characteristics of the node. The actual limit is indicated in the tmnxSub NotifNumber object.
Effect	The system cannot maintain accumulated statistics for one or more subscribers; when the subscriber hosts become idle and the system destroys the subscriber context, the statistics are also destroyed.
Recovery	If the situation is judged unacceptable, resources can be made available and the configuration can be changed to restrict the number of subscribers that require accumulated statistics. Resources can be made available (temporarily) by identifying inactive subscribers and clearing their statistics context.

76.210 tmnxSubSVlanStatsReachedMaximum

Table 1727: tmnxSubSVlanStatsReachedMaximum properties

Property name	Value
Application name	SVCMGR
Event ID	2577

Property name	Value
Event name	tmnxSubSVlanStatsReachedMaximum
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.50
Default severity	warning
Source stream	main
Message format string	The number of entries in the Subscriber VLAN statistics table (*$tmnxSubSVlanStatsNumEntries$*) is *$tmnxSubNotifTruthValue$* its maximum.
Cause	The tmnxSubSVlanStatsReachedMaximum notification indicates if the object tmnxSubSVlanStatsNumEntries is at its maximum value. The object tmnxSubSVlanStatsNumEntries indicates the number of conceptual rows in the tmnxSubSVlanStatsTable. When the value of tmnxSubNotifTruthValue is equal to 'true', the object tmnxSubSVlan StatsNumEntries is at its maximum value. When it is 'false', the value of tmnxSubSVlanStatsNumEntries has decreased below its maximum value again.
Effect	For any additional subscriber traffic flows, no new entry will be created in the tmnxSubSVlanStatsTable, and no such statistics will be available.
Recovery	No recovery required.

76.211 tmnxSubSysChassMemoryUsageHi

Table 1728: 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
Source stream	main

Property name	Value
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.

76.212 tmnxSubUserCategoryError

Table 1729: 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
Source stream	main
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: *$tmnxSub NotifApCMapName$*. Category name: *$tmnxSubNotifApCategoryName $*. More info: *$tmnxSubAdditionalInfo$*
Cause	N/A
Effect	N/A
Recovery	N/A

76.213 tmnxSubUserCategoryOutOfCredit

Table 1730: 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
Source stream	main
Message format string	The credit has expired for host *$tmnxSubNotifIpAddr$* with MAC address *$tmnxSubNotifMacAddr$* on SAP:*$sapEncapValue$*, service:*$svcId$*. Subscriber: *$tmnxSubIdent$*. SLA Profile: *$tmnxSub NotifSLAProfName$*. Category Map name: *$tmnxSubNotifApCMap Name$*. Category name: *$tmnxSubNotifApCategoryName$*.
Cause	N/A
Effect	N/A
Recovery	N/A

76.214 tmnxSubUserCategoryRefreshCredit

Table 1731: tmnxSubUserCategoryRefreshCredit properties

Property name	Value
Application name	SVCMGR
Event ID	2529
Event name	tmnxSubUserCategoryRefreshCredit
SNMP notification prefix and OID	TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.15
Default severity	minor

Property name	Value
Source stream	main
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

76.215 tmnxSubVSubnetHostsDeleted

Table 1732: 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
Source stream	main
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.

76.216 tmnxSvcSysFdbTableHighUsgClr

Table 1733: tmnxSvcSysFdbTableHighUsgClr properties

Property name	Value
Application name	SVCMGR
Event ID	2112
Event name	tmnxSvcSysFdbTableHighUsgClr
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.91
Default severity	minor
Source stream	main
Message format string	The system FDB table usage is below 90% of the system FDB table size, Current usage = *$tmnxSvcSysFdbAllocEntries$*
Cause	The tmnxSvcSysFdbTableHighUsgClr notification is generated when the system FDB table usage drops below 90% of the system FDB table size.
Effect	The system FDB table usage is below 90% of system FDB table size.
Recovery	None needed.

76.217 tmnxSvcSysFdbTableHighUsgSet

Table 1734: tmnxSvcSysFdbTableHighUsgSet properties

Property name	Value
Application name	SVCMGR
Event ID	2107
Event name	tmnxSvcSysFdbTableHighUsgSet
SNMP notification prefix and OID	TIMETRA-SERV-MIB.svcTraps.90
Default severity	minor
Source stream	main

Property name	Value
Message format string	The system FDB table usage is above 95% of the system FDB table size, Current usage = *$tmnxSvcSysFdbAllocEntries$*
Cause	The tmnxSvcSysFdbTableHighUsgSet notification is generated when the system FDB table usage exceeds 95% of the system FDB table size.
Effect	The system FDB table usage is above 95% of system FDB table size.
Recovery	None needed.

77 SYSTEM

77.1 mdCommitInProgress

Table 1735: mdCommitInProgress properties

Property name	Value
Application name	SYSTEM
Event ID	2120
Event name	mdCommitInProgress
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	Commit by *$userName$* (*$interface$*) from *$srcAddr$* is taking longer than expected - *$reason$*.
Cause	The mdCommitInProgress event is generated when a commit that is in progress on a model-driven interface is taking longer than expected to finish.
Effect	Additional commands may not be entered while the commit is in progress, and the session that issued the commit will wait until it finishes.
Recovery	No recovery is necessary.

77.2 mdCommitSucceeded

Table 1736: mdCommitSucceeded properties

Property name	Value
Application name	SYSTEM
Event ID	2121

Property name	Value
Event name	mdCommitSucceeded
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	Commit to *$regionName$* by *$userName$* (*$interface$*) from *$srcAddr $* succeeded.
Cause	The mdCommitSucceeded event is generated when a commit succeeded.
Effect	The commit succeeded.
Recovery	No recovery is necessary.

77.3 mdSaveCommitHistoryFailed

Table 1737: mdSaveCommitHistoryFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2087
Event name	mdSaveCommitHistoryFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.91
Default severity	major
Source stream	main
Message format string	*$regionName$* commit history file write failed: *$fileName$*
Cause	Saving the commit history file failed because of an error.
Effect	The commit history file was not saved.
Recovery	Identify the cause of the failure and save the configuration to save the commit history.

77.4 persistenceRestoreProblem

Table 1738: 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
Source stream	main
Message format string	Problem occurred while processing persistence record for *$tmnx PersistencyClient$ - $tmnxPersistencyNotifyMsg$*
Cause	The persistenceRestoreProblem notification is generated when an error is detected while processing a persistence record.
Effect	N/A
Recovery	N/A

77.5 persistencyClosedAlarmCleared

Table 1739: 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
Source stream	main

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

77.6 persistencyClosedAlarmRaised

Table 1740: 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
Source stream	main
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

77.7 persistencyEventReport

Table 1741: persistencyEventReport properties

Property name	Value
Application name	SYSTEM
Event ID	2037
Event name	persistencyEventReport
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.37
Default severity	warning
Source stream	main
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

77.8 persistencyFileSysThresCleared

Table 1742: 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
Source stream	main
Message format string	Filesystem on Card *$tmnxPersistenceAffectedCpm$* for *$tmnx PersistencyClient$* on device *$tmnxPersistencyFileLocator$* has dropped below threshold level of 90 percent. *$tmnxPersistencyNotify Msg$*

Property name	Value
Cause	The persistencyFileSysThresCleared notification is generated when the filesystem drops below 90 percent occupation.
Effect	N/A
Recovery	N/A

77.9 persistencyFileSysThresRaised

Table 1743: 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
Source stream	main
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

77.10 sbiBootConfig

Table 1744: sbiBootConfig properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2004
Event name	sbiBootConfig
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.4
Default severity	major
Source stream	main
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
Recovery	No recovery is necessary.

77.11 sbiBootConfigFailFileError

Table 1745: 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
Source stream	main
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.

77.12 sbiBootConfigOKFileError

Table 1746: 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
Source stream	main
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
Recovery	No recovery is necessary.

77.13 sbiBootMdReadCommitHistoryFailed

Table 1747: sbiBootMdReadCommitHistoryFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2088
Event name	sbiBootMdReadCommitHistoryFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.92
Default severity	major
Source stream	main
Message format string	*$regionName$* commit history file read failed: *$fileName$*
Cause	Reading the commit history file failed because of an error.

Property name	Value
Effect	The commit history file was not read.
Recovery	Identify the cause of the failure and reboot the system.

77.14 sbiBootSnmpd

Table 1748: 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
Source stream	main
Message format string	SNMP daemon initialization complete. System configured with persistent SNMP indexes: *$sbiPersistIndex$*. SNMP daemon administrative 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.

77.15 schedActionFailure

Table 1749: 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
Source stream	main
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

77.16 smScriptAbort

Table 1750: 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
Source stream	main
Message format string	The *$tmnxSmRunExtAuthType$* operation failed or was aborted with error: *$smRunError$*. Run # *$smRunIndex$* of script-policy "*$sm LaunchName$*" created by owner "*$smLaunchOwner$*" was executed with the user account " *$tmnxSmRunExtUserName$*".

Property name	Value
Cause	A running script terminated with an smRunExitCode not equal to `no Error'.
Effect	N/A
Recovery	N/A

77.17 smScriptException

Table 1751: smScriptException properties

Property name	Value
Application name	SYSTEM
Event ID	2104
Event name	smScriptException
SNMP notification prefix and OID	DISMAN-SCRIPT-MIB.smTraps.3
Default severity	minor
Source stream	main
Message format string	The *$tmnxSmRunExtAuthType$* operation completed with an exception: *$smRunError$*. Run *#$smRunIndex$* of script-policy " *$smLaunchName$*" 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

77.18 smScriptResult

Table 1752: 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
Source stream	main
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
Recovery	N/A

77.19 sntpTimeDiffExceedsThreshold

Table 1753: 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
Source stream	main

Property name	Value
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

77.20 socket_bind_failed

Table 1754: 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
Source stream	main
Message format string	Could not bind to a socket
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.

77.21 socket_conn_accept_failed

Table 1755: 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
Source stream	main
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.

77.22 ssiSaveBackgroundConfigFailed

Table 1756: ssiSaveBackgroundConfigFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2113
Event name	ssiSaveBackgroundConfigFailed
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	main
Message format string	Complete configuration file background write failed: *$fileName$ $reason$*
Cause	A background complete configuration save was initiated by the system to aggregate incremental saved configuration file.
Effect	The complete configuration file could not be saved.

Property name	Value
Recovery	Identify the cause of the failure and save the configuration.

77.23 ssiSaveBackgroundConfigSucceeded

Table 1757: ssiSaveBackgroundConfigSucceeded properties

Property name	Value
Application name	SYSTEM
Event ID	2112
Event name	ssiSaveBackgroundConfigSucceeded
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	Complete configuration file saved in the background to: *$fileName$*
Cause	A background complete configuration save was initiated by the system to aggregate incremental saved configuration files.
Effect	The complete configuration file was saved.
Recovery	No recovery is necessary.

77.24 ssiSaveConfigFailed

Table 1758: ssiSaveConfigFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2003
Event name	ssiSaveConfigFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.3

Property name	Value
Default severity	major
Source stream	main
Message format string	Configuration file write failed: *$fileName$ $reason$*
Cause	Saving the configuration failed because of an error.
Effect	The configuration was not saved.
Recovery	Identify the cause of the failure and save the configuration.

77.25 ssiSaveConfigSucceeded

Table 1759: 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	warning
Source stream	main
Message format string	Configuration file saved to: *$fileName$*
Cause	Saving the configuration succeeded.
Effect	The configuration was saved.
Recovery	No recovery is necessary.

77.26 ssiSaveIncrementConfigFailed

Table 1760: ssiSaveIncrementConfigFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2111
Event name	ssiSaveIncrementConfigFailed
SNMP notification prefix and OID	N/A
Default severity	major
Source stream	main
Message format string	Incremental configuration file write failed: *$fileName$ $reason$*
Cause	An incremental configuration save was initiated.
Effect	The incremental configuration file could not be saved.
Recovery	Identify the cause of the failure and save the configuration.

77.27 ssiSaveIncrementConfigSucceeded

Table 1761: ssiSaveIncrementConfigSucceeded properties

Property name	Value
Application name	SYSTEM
Event ID	2110
Event name	ssiSaveIncrementConfigSucceeded
SNMP notification prefix and OID	N/A
Default severity	warning
Source stream	main
Message format string	Incremental configuration file saved to: *$fileName$*
Cause	An incremental configuration save was initiated.
Effect	The incremental configuration file was saved.
Recovery	No recovery is necessary.

77.28 ssiSyncBootEnvFailed

Table 1762: 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
Source stream	main
Message format string	Synchronization of boot environment files failed - *$tmnxSyncFailureReason$*
Cause	The synchronization of boot environment files was stopped due to errors.
Effect	Boot environment files were not synchronized.
Recovery	No recovery is necessary.

77.29 ssiSyncBootEnvOK

Table 1763: 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
Source stream	main
Message format string	Boot environment files have been successfully synchronized

Property name	Value
Cause	The synchronization of boot environment files finished without errors.
Effect	Boot environment files were synchronized.
Recovery	No recovery is necessary.

77.30 ssiSyncCertFailed

Table 1764: ssiSyncCertFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2049
Event name	ssiSyncCertFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.49
Default severity	major
Source stream	main
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.

77.31 ssiSyncCertOK

Table 1765: ssiSyncCertOK properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2048
Event name	ssiSyncCertOK
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.48
Default severity	warning
Source stream	main
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.

77.32 ssiSyncConfigFailed

Table 1766: ssiSyncConfigFailed properties

Property name	Value
Application name	SYSTEM
Event ID	2013
Event name	ssiSyncConfigFailed
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.15
Default severity	critical
Source stream	main
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.

77.33 ssiSyncConfigOK

Table 1767: 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
Source stream	main
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.

77.34 ssiSyncRollbackFailed

Table 1768: 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
Source stream	main
Message format string	Synchronization of rollback file(s) failed - *$tmnxSyncFailureReason$*

Property name	Value
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.

77.35 ssiSyncRollbackOK

Table 1769: 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
Source stream	main
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.
Recovery	No recovery is necessary.

77.36 stiDateAndTimeChanged

Table 1770: 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
Source stream	main
Message format string	Date and time on the system is *$stiDateAndTime$*
Cause	The stiDateAndTimeChanged notification is generated when the time on the system is explicitly set.
Effect	The time on the system has been modified.
Recovery	No recovery is necessary.

77.37 stiDateAndTimeChanging

Table 1771: 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
Source stream	main
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 that the time of the change can be related to the original timescale. It shall be followed by the stiDateAndTimeChanged notification.

Property name	Value
Effect	The time on the system is being changed.
Recovery	No recovery is necessary.

77.38 tMirrorLiXIfLicenseInvalid

Table 1772: tMirrorLiXIfLicenseInvalid properties

Property name	Value
Application name	SYSTEM
Event ID	2086
Event name	tMirrorLiXIfLicenseInvalid
SNMP notification prefix and OID	TIMETRA-MIRROR-MIB.tMirrorNotifications.30
Default severity	minor
Source stream	main
Message format string	TCP LI license invalid; please remove x-interface configuration*$tMirrorLiNotifyLongDescription$*
Cause	The system sends a tMirrorLiXIfLicenseInvalid notification when x-interfaces configuration is made while the system license does not support such configuration.
Effect	The values of the objects tMirrorLiX1OperState, tMirrorLiX1OperState and tMirrorLiX1OperState remain 'outOfService'.
Recovery	Remove any X-interfaces configuration.

77.39 tmnxConfigConflict

Table 1773: tmnxConfigConflict properties

Property name	Value
Application name	SYSTEM
Event ID	2058

Property name	Value
Event name	tmnxConfigConflict
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.58
Default severity	warning
Source stream	main
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.

77.40 tmnxConfigCreate

Table 1774: tmnxConfigCreate properties

Property name	Value
Application name	SYSTEM
Event ID	2007
Event name	tmnxConfigCreate
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9
Default severity	warning
Source stream	change
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

77.41 tmnxConfigDelete

Table 1775: 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
Source stream	change
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

77.42 tmnxConfigModify

Table 1776: tmnxConfigModify properties

Property name	Value
Application name	SYSTEM
Event ID	2006
Event name	tmnxConfigModify
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.8

Property name	Value
Default severity	warning
Source stream	change
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 an NMS to trigger maintenance polls of the configuration information. Although this log event is primarily associated with classic management interfaces (for example, Classic CLI or SNMP), it is also generated when configuration changes are committed using model driven interfaces (for example, MD-CLI or NETCONF).
Effect	N/A
Recovery	No recovery is necessary.

77.43 tmnxEhsDroppedByMinDelay

Table 1777: 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
Source stream	main
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 within the time period specified by tmnxEhsHEntryMinDelay.

Property name	Value
Effect	The value of tmnxEhsHEntryStatsErrMinDelay gets incremented. Execution of the script policy stops.
Recovery	No recovery is necessary.

77.44 tmnxEhsHandlerInvoked

Table 1778: 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
Source stream	main
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.

77.45 tmnxFtpClientFailure

Table 1779: tmnxFtpClientFailure properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2034
Event name	tmnxFtpClientFailure
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.34
Default severity	minor
Source stream	main
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

77.46 tmnxLastSystemRebootAdmin

Table 1780: tmnxLastSystemRebootAdmin properties

Property name	Value
Application name	SYSTEM
Event ID	2114
Event name	tmnxLastSystemRebootAdmin
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.74
Default severity	minor
Source stream	main
Message format string	A reboot was administratively triggered at *$tmnxLastSystemReboot Time$* by user *$tmnxLastSystemRebootUser$* from *$tmnxLastSystem RebootUserAddress$*
Cause	The tmnxLastSystemRebootAdmin notification is generated when the reason for the last system reboot (as indicated by tmnxLastSystem RebootReason) was 'admin (1)'.
Effect	No effect.
Recovery	No recovery is necessary.

77.47 tmnxModuleMallocFailed

Table 1781: 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
Source stream	main
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

77.48 tmnxRedCpmActive

Table 1782: 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
Source stream	main

Property name	Value
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.
Effect	N/A
Recovery	N/A

77.49 tmnxRedSingleCpm

Table 1783: 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
Source stream	main
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

77.50 tmnxRedStandbyReady

Table 1784: tmnxRedStandbyReady properties

Property name	Value
Application name	SYSTEM
Event ID	2025
Event name	tmnxRedStandbyReady
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.25
Default severity	major
Source stream	main
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

77.51 tmnxRedStandbySyncing

Table 1785: 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
Source stream	main

Property name	Value
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

77.52 tmnxRedStandbySyncLost

Table 1786: 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
Source stream	main
Message format string	Redundancy synchronization with standby CPM card *$cpmSlotName$* has been lost.
Cause	The active CPM lost communication with the standby CPM.
Effect	N/A
Recovery	N/A

77.53 tmnxRedSwitchover

Table 1787: 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
Source stream	main
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

77.54 tmnxSmLaunchStartFailed

Table 1788: 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
Source stream	main
Message format string	Launch of *$tmnxSmRunExtAuthType$* operation failed with 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

Property name	Value
	and smLaunchScriptName don't have an existing entry in the smScript Table. 2. The value of smScriptOperStatus is not 'enabled'. 3. The sm ScriptSource 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 sm LaunchMaxRunning.
Effect	The result is indicated by incrementing the value of tmnxEhsHEntry StatsErrLaunch.
Recovery	No recovery is necessary.

77.55 tmnxSnmpdStateChange

Table 1789: 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
Source stream	main
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 administrative or operational state of the SNMP agent.
Effect	N/A
Recovery	N/A

77.56 tmnxSntpOperChange

Table 1790: 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
Source stream	main
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

77.57 tmnxSssiMismatch

Table 1791: tmnxSssiMismatch properties

Property name	Value
Application name	SYSTEM
Event ID	2022
Event name	tmnxSssiMismatch
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.22
Default severity	major
Source stream	main
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.

Property name	Value
Effect	Boot environment files are not synchronized. Following a system failover, SNMP indexes may not have the same values.
Recovery	Enable synchronization.

77.58 tmnxStateChange

Table 1792: 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
Source stream	change
Message format string	Status of *$tmnxNotifyObjectName$* changed administrative state: *$tmnxNotifyRowAdminState$*, operational state: *$tmnxNotifyRowOperState$*
Cause	A change occurred in either the administrative or operational state of a MIB table entry.
Effect	N/A
Recovery	No recovery is necessary.

77.59 tmnxSysAppStats24HrsAvailable

Table 1793: tmnxSysAppStats24HrsAvailable properties

Property name	Value
Application name	SYSTEM
Event ID	2071

Property name	Value
Event name	tmnxSysAppStats24HrsAvailable
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.72
Default severity	warning
Source stream	main
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.

77.60 tmnxSysAppStatsWeekAvailable

Table 1794: 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
Source stream	main
Message format string	New rows are available in the tmnxSysAppStatsWeekTable containing values collected at *$tmnxSysNotifAppStatsTime$*

Property name	Value
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.

77.61 tmnxSysBaseMacAddressNotSet

Table 1795: 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
Source stream	main
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.

77.62 tmnxSysDyingGasp

Table 1796: tmnxSysDyingGasp properties

Property name	Value
Application name	SYSTEM
Event ID	2090
Event name	tmnxSysDyingGasp
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.93
Default severity	critical
Source stream	main
Message format string	System is going down
Cause	The tmnxSysDyingGasp notification is sent when the system goes down due to power loss. The system attempts to send this trap using the power remaining in the dying gasp capacitor.
Effect	System goes down.
Recovery	Restore power at site.

77.63 tmnxSysExecFinished

Table 1797: tmnxSysExecFinished properties

Property name	Value
Application name	SYSTEM
Event ID	2053
Event name	tmnxSysExecFinished
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.53
Default severity	major
Source stream	main
Message format string	Possible messages: • The CLI user initiated '*$tmnxLogExecRollbackOpType$*' operation to process the commands in the SR OS CLI file *$tmnxSysExecScript$* has completed with the result of *$tmnxSysExecResult$*

Property name	Value
	• 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."

77.64 tmnxSysExecStarted

Table 1798: tmnxSysExecStarted properties

Property name	Value
Application name	SYSTEM
Event ID	2052
Event name	tmnxSysExecStarted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.52
Default severity	major
Source stream	main
Message format string	Possible messages: • A CLI user has initiated an '*$tmnxLogExecRollbackOpType$*' operation to process the commands in the SR OS CLI file *$tmnxSysExecScript$*

Property name	Value
	• Processing of '*$tmnxLogExecRollbackOpType$*' configuration messages has been initiated
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.

77.65 tmnxSysHttpRdrOutOfSeqLimitExc

Table 1799: tmnxSysHttpRdrOutOfSeqLimitExc properties

Property name	Value
Application name	SYSTEM
Event ID	2091
Event name	tmnxSysHttpRdrOutOfSeqLimitExc
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.94
Default severity	warning
Source stream	main
Message format string	More than 10 out-of-sequence TCP packets received for TCP connection *$tmnxSysAdditionalInfo$*
Cause	The notification tmnxSysHttpRdrOutOfSeqLimitExc is sent when the value of the object tmnxSysHttpRdrCpmOptimizedMode is equal to 'true' and, for any given HTTP relay TCP connection, the number of -

Property name	Value
	TCP sync packets (receive direction) or - TCP data packets (transmit direction) received out-of-sequence exceeds the limit of 10.
Effect	The out-of-sequence packets received for that connection are dropped.
Recovery	The root cause in the network must be found and fixed.

77.66 tmnxSysMgmtIfLiCfgNotEncrypted

Table 1800: tmnxSysMgmtIfLiCfgNotEncrypted properties

Property name	Value
Application name	SYSTEM
Event ID	2080
Event name	tmnxSysMgmtIfLiCfgNotEncrypted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.83
Default severity	minor
Source stream	main
Message format string	li.cfg has failed to load at bootup, system expected the li.cfg to be encrypted
Cause	The tmnxSysMgmtIfLiCfgNotEncrypted notification is generated when the Lawful Intercept (LI) configuration file is not encrypted.
Effect	The Lawful Intercept (LI) configuration file is not loaded during the boot.
Recovery	Reboot with the correct Lawful Intercept (LI) configuration file

77.67 tmnxSysMgmtIfLiIncorrectFormat

Table 1801: tmnxSysMgmtIfLiIncorrectFormat properties

Property name	Value
Application name	SYSTEM

Property name	Value
Event ID	2079
Event name	tmnxSysMgmtIfLiIncorrectFormat
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.82
Default severity	minor
Source stream	main
Message format string	LI config failed to load. The LI config is in the format '$sbiPrimary ConfigFileFormatType' and can only load if it matches the format of the primary configuration file '$sbiLiConfigFileFormatType'
Cause	The tmnxSysMgmtIfLiIncorrectFormat notification is generated when a format (classic or model-driven) of the Lawful Intercept (LI) configuration file does not match primary configuration file format.
Effect	The Lawful Intercept (LI) configuration file is not loaded during the boot.
Recovery	Reboot with the correct Lawful Intercept (LI) configuration file

77.68 tmnxSysMgmtIfModeChangeComplete

Table 1802: tmnxSysMgmtIfModeChangeComplete properties

Property name	Value
Application name	SYSTEM
Event ID	2077
Event name	tmnxSysMgmtIfModeChangeComplete
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.79
Default severity	major
Source stream	main
Message format string	Management interface configuration mode change to *$tmnxSysMgmtIfWriteMode$* has completed.
Cause	The tmnxSysMgmtIfModeChangeComplete notification is generated when a management interface configuration mode change request is complete.

Property name	Value
Effect	Switching modes between any configuration mode will lock the configuration datastores from operator input until the mode switch has completed. Once this event is triggered the configuration datastores are unlocked for operator input.
Recovery	None.

77.69 tmnxSysMgmtIfModeChangeFailure

Table 1803: tmnxSysMgmtIfModeChangeFailure properties

Property name	Value
Application name	SYSTEM
Event ID	2078
Event name	tmnxSysMgmtIfModeChangeFailure
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.80
Default severity	major
Source stream	main
Message format string	Management interface configuration mode change failed. The system is now in *$tmnxSysMgmtIfWriteMode$* mode
Cause	The tmnxSysMgmtIfModeChangeFailure notification is generated when a management interface configuration mode change request fails to complete.
Effect	Switching modes between any configuration mode will lock the configuration datastores from operator input until the mode switch has completed. When this event is triggered the mode change is declared unsuccessful; the effective configuration mode will be indicated in this notification. The configuration datastores are unlocked for operator input.
Recovery	None.

77.70 tmnxSysMgmtIfModeChangeStart

Table 1804: tmnxSysMgmtIfModeChangeStart properties

Property name	Value
Application name	SYSTEM
Event ID	2076
Event name	tmnxSysMgmtIfModeChangeStart
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.78
Default severity	major
Source stream	main
Message format string	A management interface configuration mode change (reason *$tmnxSysMgmtIfWriteSwitchReason$*) from *$tmnxNotifySysMgmtIfOriginalMode$* to *$tmnxSysMgmtIfWriteMode$* was initiated.
Cause	The tmnxSysMgmtIfModeChangeStart notification is generated when a management interface configuration mode change request is sent.
Effect	Switching modes between any configuration mode will lock the configuration datastores from operator input until the mode switch has completed.
Recovery	None.

77.71 tmnxSysNvsysFileError

Table 1805: 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
Source stream	main
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.

77.72 tmnxSysRollbackDeleteStarted

Table 1806: 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
Source stream	main
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 tmnxSysRollbackIndex and tmnxSysRollbackFileType.
Effect	The specified configuration file is deleted.
Recovery	There is no recovery required for this notification.

77.73 tmnxSysRollbackFileDeleteStatus

Table 1807: tmnxSysRollbackFileDeleteStatus properties

Property name	Value
Application name	SYSTEM
Event ID	2045
Event name	tmnxSysRollbackFileDeleteStatus
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.45
Default severity	minor
Source stream	main
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.

77.74 tmnxSysRollbackSaveStarted

Table 1808: 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
Source stream	main
Message format string	Rollback save of file *$fileName$* started

Property name	Value
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.

77.75 tmnxSysRollbackSaveStatusChange

Table 1809: 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
Source stream	main
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 failed, the user should try to determine the reason for the failure. The user can attempt a recovery by attempting the rollback save again.

77.76 tmnxSysRollbackStarted

Table 1810: 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
Source stream	main
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.
Recovery	There is no recovery required for this notification.

77.77 tmnxSysRollbackStatusChange

Table 1811: 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
Source stream	main
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.

Property name	Value
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.

77.78 tmnxSysSwFabFailRecAborted

Table 1812: tmnxSysSwFabFailRecAborted properties

Property name	Value
Application name	SYSTEM
Event ID	2084
Event name	tmnxSysSwFabFailRecAborted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.89
Default severity	major
Source stream	main
Message format string	Automatic switch fabric failure recovery aborted
Cause	The tmnxSysSwFabFailRecAborted notification is generated when the automatic switch fabric recovery process was aborted.
Effect	This may have been due to a problem with one of the SFMs resetting and may have left the router with reduced switch fabric capacity.
Recovery	Check to ensure all SFMs are fully operational. For any SFMs that are not operational, investigate manual recovery.

77.79 tmnxSysSwFabFailRecCompleted

Table 1813: tmnxSysSwFabFailRecCompleted properties

Property name	Value
Application name	SYSTEM
Event ID	2083
Event name	tmnxSysSwFabFailRecCompleted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.88
Default severity	cleared
Source stream	main
Message format string	Automatic switch fabric failure recovery completed
Cause	The tmnxSysSwFabFailRecCompleted notification is generated when the automatic switch fabric recovery process has completed successfully.
Effect	The switch fabric has been returned to normal operation.
Recovery	No recovery is necessary.

77.80 tmnxSysSwFabFailRecDetected

Table 1814: tmnxSysSwFabFailRecDetected properties

Property name	Value
Application name	SYSTEM
Event ID	2085
Event name	tmnxSysSwFabFailRecDetected
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.90
Default severity	major
Source stream	main
Message format string	Automatic switch fabric failure recovery triggered
Cause	The tmnxSysSwFabFailRecDetected notification is generated when a condition has been detected within the router that might be resolved by the running of the automatic switch fabric recovery process.

Property name	Value
Effect	If the automatic switch faric recovery process is enabled and all the required prerequisites are met, then the recovery process will start. If the automatic process is enabled but the recovery does not start, then the prerequisite conditions should be checked to determine what needs to be corrected to allow the process to run.
Recovery	No recovery is necessary.

77.81 tmnxSysSwFabFailRecStarted

Table 1815: tmnxSysSwFabFailRecStarted properties

Property name	Value
Application name	SYSTEM
Event ID	2082
Event name	tmnxSysSwFabFailRecStarted
SNMP notification prefix and OID	TIMETRA-SYSTEM-MIB.tmnxSysNotifications.87
Default severity	major
Source stream	main
Message format string	Automatic switch fabric failure recovery started
Cause	The tmnxSysSwFabFailRecStarted notification is generated when the router has initiated an automatic switch fabric recovery process based on detecting frequent failures to multiple IOM/XCMs. Such multiple failures could be caused by issues on the SFM so this process involves the sequential reset of the SFMs to attempt to clear the cause of the failures.
Effect	The router shall operate at reduced switch fabric capacity while each individual SFM is reset in turn.
Recovery	This process will run until all the SFMs have been processed. No recovery is necessary.

77.82 tmnxTrapDropped

Table 1816: 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
Source stream	main
Message format string	Possible messages: • Dropped notification *$tmnxDroppedTrapName$* for *$tmnxDroppedTrapEntryName$* because of *$tmnxTrapDroppedReasonCode$* • 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

78 TLS

78.1 tmnxTlsFailure

Table 1817: 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
Source stream	security
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.

78.2 tmnxTlsInitiateSession

Table 1818: tmnxTlsInitiateSession properties

Property name	Value
Application name	TLS

Property name	Value
Event ID	2001
Event name	tmnxTlsInitiateSession
SNMP notification prefix and OID	TIMETRA-TLS-MIB.tmnxTlsNotifications.1
Default severity	minor
Source stream	security
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.

78.3 tmnxTlsTermination

Table 1819: 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
Source stream	security
Message format string	TLS session terminated for application *$tmnxTlsAppId$ $tmnxTlsRole $* router instance *$tmnxTlsVRtrID$* source address *$tmnxTlsLocalAddr $* sourcePort *$tmnxTlsLocalPort$* destination address *$tmnxTlsRemote Addr$* destinationPort *$tmnxTlsRemotePort$*

Property name	Value
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.

79 TREE_SID

79.1 vRtrTreeSidCdtPathActInsChanged

Table 1820: vRtrTreeSidCdtPathActInsChanged properties

Property name	Value
Application name	TREE_SID
Event ID	2002
Event name	vRtrTreeSidCdtPathActInsChanged
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.2
Default severity	minor
Source stream	main
Message format string	Switched candidate-path(*$vRtrTreeSidDBPlcyCdtPathName$*) active-instance from (*$vRtrTreeSidDBPlcyCPOldActiveInst$*) to (*$vRtrTree SidDBPlcyCPActiveInst$*) for p2mp-policy.
Cause	Generated when the active instance for a candidate-path changes from vRtrTreeSidDBPlcyCPOldActiveInst to vRtrTreeSidDBPlcyCPActive Inst;
Effect	Switching to the new active-instance for the candidate-path was successful.
Recovery	None required.

79.2 vRtrTreeSidCdtPathChanged

Table 1821: vRtrTreeSidCdtPathChanged properties

Property name	Value
Application name	TREE_SID
Event ID	2001

Property name	Value
Event name	vRtrTreeSidCdtPathChanged
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.1
Default severity	minor
Source stream	main
Message format string	Switched candidate-path from (*$vRtrTreeSidDBPlcyOldCdtPathName$*) to (*$vRtrTreeSidDBPlcyCdtPathName$*) for p2mp-policy .
Cause	Generated when the in-use candidate-path changes from vRtrTree SidDBPlcyOldCdtPathName to vRtrTreeSidDBPlcyCdtPathName;
Effect	Switching to the new candidate-path was successful.
Recovery	None Required.

79.3 vRtrTreeSidFailOverPriToStdBy

Table 1822: vRtrTreeSidFailOverPriToStdBy properties

Property name	Value
Application name	TREE_SID
Event ID	2009
Event name	vRtrTreeSidFailOverPriToStdBy
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.9
Default severity	minor
Source stream	main
Message format string	Traffic switched for MVPN instance *$vRtrID$* from primary PE *$vRtrPimNgMvpnUMHPEAddr$* to standby PE *$vRtrPim NgMvpnUMHPEStandbyAddr$* due to *$vRtrTreeSidFailOverReason Code$*
Cause	The vRtrTreeSidFailOverPriToStdBy 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.

Property name	Value
Recovery	None required.

79.4 vRtrTreeSidFailOverStdByToPri

Table 1823: vRtrTreeSidFailOverStdByToPri properties

Property name	Value
Application name	TREE_SID
Event ID	2010
Event name	vRtrTreeSidFailOverStdByToPri
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.10
Default severity	minor
Source stream	main
Message format string	Traffic switched for MVPN instance *$vRtrID$* from standby PE *$vRtrPimNgMvpnUMHPEStandbyAddr$* to primary PE *$vRtrPimNgMvpnUMHPEAddr$*
Cause	The vRtrTreeSidFailOverStdByToPri 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 vRtrPimNgMvpnUMHPEAddrType and vRtrPimNgMvpnUMHPEAddr indexes of the varbinds in this notification.
Effect	The tunnel traffic may be affected.
Recovery	None required.

79.5 vRtrTreeSidInSidRegFailure

Table 1824: vRtrTreeSidInSidRegFailure properties

Property name	Value
Application name	TREE_SID
Event ID	2003

Property name	Value
Event name	vRtrTreeSidInSidRegFailure
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.3
Default severity	minor
Source stream	main
Message format string	Incoming SID registration failed for replication-segment.
Cause	Reports a failure while programming an incoming-sid specified by vRtr TreeSidDBRplPlcyIncomingSid.
Effect	Programming of the replication-segment failed.
Recovery	Configuration change, using a different incoming-sid.

79.6 vRtrTreeSidLabelRangeExhaustion

Table 1825: vRtrTreeSidLabelRangeExhaustion properties

Property name	Value
Application name	TREE_SID
Event ID	2007
Event name	vRtrTreeSidLabelRangeExhaustion
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.7
Default severity	minor
Source stream	main
Message format string	MPLS reserved-label-block range exhausted. System will not accept new replication-segment configuration with pop and swap operation.
Cause	Generated when the reserved-label range for p2mp-sr-tree is exhausted.
Effect	System may not accept new replication-segment configuration with pop and swap operation.
Recovery	Configuration change may be required.

79.7 vRtrTreeSidLblRangeExhstCleared

Table 1826: vRtrTreeSidLblRangeExhstCleared properties

Property name	Value
Application name	TREE_SID
Event ID	2008
Event name	vRtrTreeSidLblRangeExhstCleared
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.8
Default severity	minor
Source stream	main
Message format string	MPLS reserved-label-block range exhaustion cleared.
Cause	Generated when an earlier label range exhaustion condition raised by v RtrTreeSidLabelRangeExhaustion is cleared.
Effect	System can accept new replication-segment configuration with pop and swap operation.
Recovery	None required.

79.8 vRtrTreeSidRepSegResExhaustion

Table 1827: vRtrTreeSidRepSegResExhaustion properties

Property name	Value
Application name	TREE_SID
Event ID	2005
Event name	vRtrTreeSidRepSegResExhaustion
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.5
Default severity	minor
Source stream	main

Property name	Value
Message format string	(*$vRtrTreeSidResourceType$*) resource exhausted for replication-segment with root-addr(*$vRtrTreeSidDBReplPlcyRootAddr$*), tree-id(*$vRtrTreeSidDBReplPlcyTreeId$*), instance-id(*$vRtrTreeSidDBReplPlcyInstanceId$*), origin(*$vRtrTreeSidDBReplPlcyOrigin$*).
Cause	Generated when a CPM or data path resource specified by vRtrTreeSidResourceType cannot be allocated for the replication-segment.
Effect	The replication segment will be operationally down.
Recovery	Configuration change may be required. May be cleared while retrying for the exhausted resource.

79.9 vRtrTreeSidRepSegResExhstCleared

Table 1828: vRtrTreeSidRepSegResExhstCleared properties

Property name	Value
Application name	TREE_SID
Event ID	2006
Event name	vRtrTreeSidRepSegResExhstCleared
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.6
Default severity	minor
Source stream	main
Message format string	(*$vRtrTreeSidResourceType$*) resource exhaustion cleared for replication-segment with root-addr(*$vRtrTreeSidDBReplPlcyRootAddr$*), tree-id(*$vRtrTreeSidDBReplPlcyTreeId$*), instance-id(*$vRtrTreeSidDBReplPlcyInstanceId$*), origin(*$vRtrTreeSidResourceType$*).
Cause	Generated when an earlier resource exhaustion condition raised by vRtrTreeSidRepSegResExhaustion is cleared.
Effect	CPM or data path resource specified by vRtrTreeSidResourceType can be allocated now for the replication-segment.
Recovery	None required.

79.10 vRtrTreeSidTreeIdAllocFailure

Table 1829: vRtrTreeSidTreeIdAllocFailure properties

Property name	Value
Application name	TREE_SID
Event ID	2004
Event name	vRtrTreeSidTreeIdAllocFailure
SNMP notification prefix and OID	TIMETRA-TREE-SID-MIB.vRtrTreeSidNotifications.4
Default severity	minor
Source stream	main
Message format string	Dynamic tree-Id allocation failed.
Cause	Generated when tree-id resource cannot be allocated.
Effect	System may not accept new replication-segment configuration
Recovery	Configuration change may be required. May also be cleared while retrying for the resource.

80 USER

80.1 cli_config_io

Table 1830: 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
Source stream	change
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	The user entered an authorized configuration command in the classic CLI.
Effect	The configuration was changed by the CLI command.
Recovery	No recovery is required

80.2 cli_unauth_config_io

Table 1831: 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

Property name	Value
Default severity	minor
Source stream	change
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	The user entered an unauthorized configuration command in the classic CLI.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

80.3 cli_unauth_user_io

Table 1832: 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
Source stream	change
Message format string	User from *$srcAddr$*. *$message$*: *$prompt$ $command$*
Cause	The user entered an unauthorized command in the classic CLI.
Effect	The CLI command was not processed.
Recovery	No recovery is required.

80.4 cli_user_io

Table 1833: 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
Source stream	change
Message format string	User from *$srcAddr$*: *$prompt$ $message$*
Cause	The user entered an authorized command in the classic CLI.
Effect	The CLI command was processed.
Recovery	No recovery is required.

80.5 cli_user_login

Table 1834: 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
Source stream	change
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.

80.6 cli_user_login_failed

Table 1835: 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
Source stream	change
Message format string	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.

80.7 cli_user_login_max_attempts

Table 1836: 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
Source stream	change
Message format string	User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in, user is locked out

Property name	Value
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.

80.8 cli_user_logout

Table 1837: 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
Source stream	change
Message format string	User from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

80.9 ftp_user_login

Table 1838: ftp_user_login properties

Property name	Value
Application name	USER
Event ID	2005

Property name	Value
Event name	ftp_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
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

80.10 ftp_user_login_failed

Table 1839: 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
Source stream	change
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.

80.11 ftp_user_login_max_attempts

Table 1840: 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
Source stream	change
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.

80.12 ftp_user_logout

Table 1841: ftp_user_logout properties

Property name	Value
Application name	USER
Event ID	2006
Event name	ftp_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	FTP user from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.

Property name	Value
Recovery	No recovery is required.

80.13 grpc_user_login

Table 1842: grpc_user_login properties

Property name	Value
Application name	USER
Event ID	2014
Event name	grpc_user_login
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	gRPC user from *$srcAddr$* logged in
Cause	A user successfully authenticated for login.
Effect	A user access session was started.
Recovery	No recovery is required

80.14 grpc_user_login_failed

Table 1843: grpc_user_login_failed properties

Property name	Value
Application name	USER
Event ID	2016
Event name	grpc_user_login_failed
SNMP notification prefix and OID	N/A
Default severity	minor

Property name	Value
Source stream	change
Message format string	gRPC 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.

80.15 grpc_user_login_max_attempts

Table 1844: grpc_user_login_max_attempts properties

Property name	Value
Application name	USER
Event ID	2017
Event name	grpc_user_login_max_attempts
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
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 gRPC session was terminated.
Recovery	No recovery is required.

80.16 grpc_user_logout

Table 1845: grpc_user_logout properties

Property name	Value
Application name	USER
Event ID	2015
Event name	grpc_user_logout
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	gRPC user from *$srcAddr$* logged out
Cause	A user logged out.
Effect	The user access session ended.
Recovery	No recovery is required.

80.17 netconf_user_login

Table 1846: 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
Source stream	change
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.

80.18 netconf_user_login_failed

Table 1847: 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
Source stream	change
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.

80.19 netconf_user_login_max_attempts

Table 1848: 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
Source stream	change
Message format string	User from *$srcAddr$* attempted more than *$maxAttempts$* times to log in, user is locked out

Property name	Value
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.

80.20 netconf_user_logout

Table 1849: 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
Source stream	change
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.

80.21 snmp_user_set

Table 1850: snmp_user_set properties

Property name	Value
Application name	USER
Event ID	2010

Property name	Value
Event name	snmp_user_set
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	change
Message format string	SNMP user from *$srcAddr$*> *$vbList$*
Cause	An SNMP SET request was received.
Effect	Configuration was changed by an SNMP SET operation.
Recovery	No recovery is required.

81 VIDEO

81.1 tmnxVdoAdSpliceAbort

Table 1851: 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
Source stream	main
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

81.2 tmnxVdoClientSessionsLmtCleared

Table 1852: tmnxVdoClientSessionsLmtCleared properties

Property name	Value
Application name	VIDEO
Event ID	2008
Event name	tmnxVdoClientSessionsLmtCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.8
Default severity	warning
Source stream	main
Message format string	Number of RTCP sessions back to the limit for client *$tmnxVdoNotify ClientAddress$*
Cause	N/A
Effect	N/A
Recovery	N/A

81.3 tmnxVdoClientSessionsLmtExceeded

Table 1853: 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
Source stream	main
Message format string	Threshold for number of RTCP sessions exceeded for client *$tmnxVdo NotifyClientAddress$*
Cause	N/A
Effect	N/A

Property name	Value
Recovery	N/A

81.4 tmnxVdoDuplicateSsrcId

Table 1854: tmnxVdoDuplicateSsrcId properties

Property name	Value
Application name	VIDEO
Event ID	2001
Event name	tmnxVdoDuplicateSsrcId
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.1
Default severity	warning
Source stream	main
Message format string	Duplicate SSRC Id *$tmnxVdoGrpSrcSSRCId$* detected: Service Id - *$svcId$*, Video interface - *$tmnxVdoIfName$*, Group address - *$tmnxVdoGrpSrcGroupAddress$*, Source address - *$tmnxVdoGrpSrcSourceAddress$*
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.

81.5 tmnxVdoGrpSrcAnlyzrErrState

Table 1855: tmnxVdoGrpSrcAnlyzrErrState properties

Property name	Value
Application name	VIDEO
Event ID	2009

Property name	Value
Event name	tmnxVdoGrpSrcAnlyzrErrState
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.9
Default severity	warning
Source stream	main
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.

81.6 tmnxVdoGrpSrcAnlyzrStClear

Table 1856: 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
Source stream	main
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.

Property name	Value
Effect	This trap is informational. No effects are caused by this trap.
Recovery	No recovery mechanism is required.

81.7 tmnxVdoMdaFccBwLimitCleared

Table 1857: tmnxVdoMdaFccBwLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2012
Event name	tmnxVdoMdaFccBwLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.12
Default severity	warning
Source stream	main
Message format string	FCC bandwidth back to the limit - *$tmnxVdoGrpMdaCurFccBw $* bandwidth on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccBwLimitCleared notification is generated after a tmnxVdoMdaFccBwLimitExceeded notification when the egress FCC (Fast Channel Change) bandwidth retreats by 10% from the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.8 tmnxVdoMdaFccBwLimitExceeded

Table 1858: tmnxVdoMdaFccBwLimitExceeded properties

Property name	Value
Application name	VIDEO

Property name	Value
Event ID	2011
Event name	tmnxVdoMdaFccBwLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.11
Default severity	warning
Source stream	main
Message format string	Threshold for FCC bandwidth exceeded - *$tmnxVdoGrpMdaCurFccBw$* bandwidth on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccBwLimitExceeded notification is generated when the egress bandwidth for FCC (Fast Channel Change) exceeds the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.9 tmnxVdoMdaFccRetTotBwLmtCleared

Table 1859: tmnxVdoMdaFccRetTotBwLmtCleared properties

Property name	Value
Application name	VIDEO
Event ID	2016
Event name	tmnxVdoMdaFccRetTotBwLmtCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.16
Default severity	warning
Source stream	main
Message format string	Total FCC and RET bandwidth back to the limit - *$tmnxVdoGrpMdaCurFccRetTotalBw$* bandwidth on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccRetTotBwLmtCleared notification is generated after a tmnxVdoMdaFccRetTotBwLmtExceeded notification when the total egress bandwidth for RET (Retransmission) and FCC (Fast Channel

Property name	Value
	Change) retreats by 10% from the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.10 tmnxVdoMdaFccRetTotBwLmtExceeded

Table 1860: tmnxVdoMdaFccRetTotBwLmtExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2015
Event name	tmnxVdoMdaFccRetTotBwLmtExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.15
Default severity	warning
Source stream	main
Message format string	Threshold for total FCC and RET bandwidth exceeded - *$tmnxVdoGrpMdaCurFccRetTotalBw$* bandwidth on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccRetTotBwLmtExceeded notification is generated when the total egress bandwidth for RET (Retransmission) and FCC (Fast Channel Change) exceeds the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.11 tmnxVdoMdaFccRetTotSeLmtCleared

Table 1861: tmnxVdoMdaFccRetTotSeLmtCleared properties

Property name	Value
Application name	VIDEO
Event ID	2022
Event name	tmnxVdoMdaFccRetTotSeLmtCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.22
Default severity	warning
Source stream	main
Message format string	Total number of FCC and RET sessions back to the limit - *$tmnxVdoGrpMdaActFccRetTotalSess$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccRetTotSeLmtCleared notification is generated after a tmnxVdoMdaFccRetTotSeLmtExceeded notification when the number of Real Time Transport Control Protocol (RTCP) sessions retreats by 10% from the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.12 tmnxVdoMdaFccRetTotSeLmtExceeded

Table 1862: tmnxVdoMdaFccRetTotSeLmtExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2021
Event name	tmnxVdoMdaFccRetTotSeLmtExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.21
Default severity	warning
Source stream	main

Property name	Value
Message format string	Threshold for total number of FCC and RET sessions exceeded - *$tmnxVdoGrpMdaActFccRetTotalSess$* sessions active on MDA *$tmnx ChassisIndex$*/*$tmnxCardSlotNum$*/ *$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccRetTotSeLmtExceeded notification is generated when the total number of Real Time Transport Control Protocol (RTCP) sessions exceeds the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.13 tmnxVdoMdaFccSesLimitCleared

Table 1863: tmnxVdoMdaFccSesLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2018
Event name	tmnxVdoMdaFccSesLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.18
Default severity	warning
Source stream	main
Message format string	Number of FCC sessions back to the limit - *$tmnxVdoGrpMdaActFcc Sess$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlot Num$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccSesLimitCleared notification is generated after a tmnxVdoMdaFccSesLimitExceeded notification when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for FCC (Fast Channel Change) retreats by 10% from the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.14 tmnxVdoMdaFccSesLimitExceeded

Table 1864: tmnxVdoMdaFccSesLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2017
Event name	tmnxVdoMdaFccSesLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.17
Default severity	warning
Source stream	main
Message format string	Threshold for number of FCC sessions exceeded - *$tmnxVdoGrpMdaActFccSess$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaFccSesLimitExceeded notification is generated when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for FCC (Fast Channel Change) exceeds the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.15 tmnxVdoMdaRetBwLimitCleared

Table 1865: tmnxVdoMdaRetBwLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2014
Event name	tmnxVdoMdaRetBwLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.14
Default severity	warning

Property name	Value
Source stream	main
Message format string	RET bandwidth back to the limit - *$tmnxVdoGrpMdaCurAbsRetBw$* bandwidth on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaRetBwLimitCleared notification is generated after a tmnxVdoMdaRetBwLimitExceeded notification when the egress RET (Retransmission) bandwidth retreats by 10% from the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.16 tmnxVdoMdaRetBwLimitExceeded

Table 1866: tmnxVdoMdaRetBwLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2013
Event name	tmnxVdoMdaRetBwLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.13
Default severity	warning
Source stream	main
Message format string	Threshold for RET bandwidth exceeded - *$tmnxVdoGrpMdaCurAbsRetBw$* bandwidth on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaRetBwLimitExceeded notification is generated when the egress bandwidth for RET (Retransmission) exceeds the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.17 tmnxVdoMdaRetSesLimitCleared

Table 1867: tmnxVdoMdaRetSesLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2020
Event name	tmnxVdoMdaRetSesLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.20
Default severity	warning
Source stream	main
Message format string	Number of RET sessions back to the limit - *$tmnxVdoGrpMdaActRetSess$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaRetSesLimitCleared notification is generated after a tmnxVdoMdaRetSesLimitExceeded notification when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for RET (Retransmission) retreats by 10% from the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.18 tmnxVdoMdaRetSesLimitExceeded

Table 1868: tmnxVdoMdaRetSesLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2019
Event name	tmnxVdoMdaRetSesLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.19

Property name	Value
Default severity	warning
Source stream	main
Message format string	Threshold for number of RET sessions exceeded - *$tmnxVdoGrpMdaActRetSess$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoMdaRetSesLimitExceeded notification is generated when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for RET (Retransmission) exceeds the high watermark level configured for a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.19 tmnxVdoMdaSessionsLimitCleared

Table 1869: 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
Source stream	main
Message format string	Number of RTCP sessions back to the limit - *$tmnxVdoGrpMdaActiveRtcpSessions$* sessions active on MDA *$tmnxChassisIndex$*/*$tmnxCardSlotNum$*/*$tmnxMDASlotNum$*, video group - *$tmnxVdoGrpId$*
Cause	This event will be generated for a video MDA when the number of active RTCP sessions are back to within the limit.
Effect	N/A
Recovery	N/A

81.20 tmnxVdoMdaSessionsLimitExceeded

Table 1870: 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
Source stream	main
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

81.21 tmnxVdoMdaSGLimitCleared

Table 1871: 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
Source stream	main
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 within the limit.
Effect	N/A
Recovery	N/A

81.22 tmnxVdoMdaSGLimitExceeded

Table 1872: 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
Source stream	main
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

81.23 tmnxVdoVappFccBwLimitCleared

Table 1873: tmnxVdoVappFccBwLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2028
Event name	tmnxVdoVappFccBwLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.28
Default severity	warning
Source stream	main
Message format string	FCC bandwidth back to the limit - *$tmnxVdoGrpVappCurFccBw$* bandwidth on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVapp Num$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccBwLimitCleared notification is generated after a tmnxVdoVappFccBwLimitExceeded notification when the egress FCC (Fast Channel Change) bandwidth retreats by 10% from the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.24 tmnxVdoVappFccBwLimitExceeded

Table 1874: tmnxVdoVappFccBwLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2027
Event name	tmnxVdoVappFccBwLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.27
Default severity	warning
Source stream	main

Property name	Value
Message format string	Threshold for FCC bandwidth exceeded - *$tmnxVdoGrpVappCurFccBw$* bandwidth on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccBwLimitExceeded notification is generated when the egress bandwidth for FCC (Fast Channel Change) exceeds the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.25 tmnxVdoVappFccRetTotBwLmtCleared

Table 1875: tmnxVdoVappFccRetTotBwLmtCleared properties

Property name	Value
Application name	VIDEO
Event ID	2032
Event name	tmnxVdoVappFccRetTotBwLmtCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.32
Default severity	warning
Source stream	main
Message format string	Total FCC and RET bandwidth back to the limit - *$tmnxVdoGrpVappCurFccRetTotalBw$* bandwidth on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccRetTotBwLmtCleared notification is generated after a tmnxVdoVappFccRetTotBwLmtExceded notification when the total egress bandwidth for RET (Retransmission) and FCC (Fast Channel Change) retreats by 10% from the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.26 tmnxVdoVappFccRetTotBwLmtExceded

Table 1876: tmnxVdoVappFccRetTotBwLmtExceded properties

Property name	Value
Application name	VIDEO
Event ID	2031
Event name	tmnxVdoVappFccRetTotBwLmtExceded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.31
Default severity	warning
Source stream	main
Message format string	Threshold for total FCC and RET bandwidth exceeded - *$tmnxVdoGrpVappCurFccRetTotalBw$* bandwidth on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccRetTotBwLmtExceded notification is generated when the total egress bandwidth for RET (Retransmission) and FCC (Fast Channel Change) exceeds the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.27 tmnxVdoVappFccRetTotSeLmtCleared

Table 1877: tmnxVdoVappFccRetTotSeLmtCleared properties

Property name	Value
Application name	VIDEO
Event ID	2038
Event name	tmnxVdoVappFccRetTotSeLmtCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.38
Default severity	warning

Property name	Value
Source stream	main
Message format string	Total number of FCC and RET sessions back to the limit - *$tmnxVdoGrpVappActFccRetTotalSess$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccRetTotSeLmtCleared notification is generated after a tmnxVdoVappFccRetTotSeLmtExceded notification when the number of Real Time Transport Control Protocol (RTCP) sessions retreats by 10% from the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.28 tmnxVdoVappFccRetTotSeLmtExceded

Table 1878: tmnxVdoVappFccRetTotSeLmtExceded properties

Property name	Value
Application name	VIDEO
Event ID	2037
Event name	tmnxVdoVappFccRetTotSeLmtExceded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.37
Default severity	warning
Source stream	main
Message format string	Threshold for total number of FCC and RET sessions exceeded - *$tmnxVdoGrpVappActFccRetTotalSess$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccRetTotSeLmtExceded notification is generated when the total number of Real Time Transport Control Protocol (RTCP) sessions exceeds the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A

Property name	Value
Recovery	N/A

81.29 tmnxVdoVappFccSesLimitCleared

Table 1879: tmnxVdoVappFccSesLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2034
Event name	tmnxVdoVappFccSesLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.34
Default severity	warning
Source stream	main
Message format string	Number of FCC sessions back to the limit - *$tmnxVdoGrpVappActFccSess$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccSesLimitCleared notification is generated after a tmnxVdoVappFccSesLimitExceeded notification when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for FCC (Fast Channel Change) retreats by 10% from the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.30 tmnxVdoVappFccSesLimitExceeded

Table 1880: tmnxVdoVappFccSesLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2033

Property name	Value
Event name	tmnxVdoVappFccSesLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.33
Default severity	warning
Source stream	main
Message format string	Threshold for number of FCC sessions exceeded - *$tmnxVdoGrpVappActFccSess$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappFccSesLimitExceeded notification is generated when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for FCC (Fast Channel Change) exceeds the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.31 tmnxVdoVappRetBwLimitCleared

Table 1881: tmnxVdoVappRetBwLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2030
Event name	tmnxVdoVappRetBwLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.30
Default severity	warning
Source stream	main
Message format string	RET bandwidth back to the limit - *$tmnxVdoGrpVappCurAbsRetBw$* bandwidth on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappRetBwLimitCleared notification is generated after a tmnxVdoVappRetBwLimitExceeded notification when the egress RET (Retransmission) bandwidth retreats by 10% from the high watermark level configured for a video Virtual Application (VAPP).

Property name	Value
Effect	N/A
Recovery	N/A

81.32 tmnxVdoVappRetBwLimitExceeded

Table 1882: tmnxVdoVappRetBwLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2029
Event name	tmnxVdoVappRetBwLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.29
Default severity	warning
Source stream	main
Message format string	Threshold for RET bandwidth exceeded - *$tmnxVdoGrpVappCurAbsRetBw$* bandwidth on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappRetBwLimitExceeded notification is generated when the egress bandwidth for RET (Retransmission) exceeds the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.33 tmnxVdoVappRetSesLimitCleared

Table 1883: tmnxVdoVappRetSesLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2036

Property name	Value
Event name	tmnxVdoVappRetSesLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.36
Default severity	warning
Source stream	main
Message format string	Number of RET sessions back to the limit - *$tmnxVdoGrpVappActRetSess$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappRetSesLimitCleared notification is generated after a tmnxVdoVappRetSesLimitExceeded notification when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for RET (Retransmission) retreats by 10% from the high watermark level configured for a video Virtual Application (VAPP).
Effect	N/A
Recovery	N/A

81.34 tmnxVdoVappRetSesLimitExceeded

Table 1884: tmnxVdoVappRetSesLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2035
Event name	tmnxVdoVappRetSesLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.35
Default severity	warning
Source stream	main
Message format string	Threshold for number of RET sessions exceeded - *$tmnxVdoGrpVappActRetSess$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappRetSesLimitExceeded notification is generated when the number of Real Time Transport Control Protocol (RTCP) sessions allocated for RET (Retransmission) exceeds the high watermark level configured for a video Virtual Application (VAPP).

Property name	Value
Effect	N/A
Recovery	N/A

81.35 tmnxVdoVappSessionsLimitCleared

Table 1885: tmnxVdoVappSessionsLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2025
Event name	tmnxVdoVappSessionsLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.25
Default severity	warning
Source stream	main
Message format string	Number of RTCP sessions back to the limit - *$tmnxVdoGrpVappActive RtcpSessions$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappSessionsLimitCleared notification is generated after a tmnxVdoVappSessionsLimitExceeded notification when the number of Real Time Transport Control Protocol (RTCP) sessions goes back down to the limit supported by a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.36 tmnxVdoVappSessionsLimitExceeded

Table 1886: tmnxVdoVappSessionsLimitExceeded properties

Property name	Value
Application name	VIDEO

Property name	Value
Event ID	2023
Event name	tmnxVdoVappSessionsLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.23
Default severity	warning
Source stream	main
Message format string	Threshold for number of RTCP sessions exceeded - *$tmnxVdoGrpVappActiveRtcpSessions$* sessions active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappSessionsLimitExceeded notification is generated when the configuration exceeds the maximum number of Real Time Transport Control Protocol (RTCP) sessions supported by a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.37 tmnxVdoVappSGLimitCleared

Table 1887: tmnxVdoVappSGLimitCleared properties

Property name	Value
Application name	VIDEO
Event ID	2026
Event name	tmnxVdoVappSGLimitCleared
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.26
Default severity	warning
Source stream	main
Message format string	Number of channels back to the limit - *$tmnxVdoGrpVappChannels$* channels active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnxVdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappSGLimitCleared notification is generated after a tmnxVdoVappSGLimitExceeded notification when the number of channels

Property name	Value
	goes back down to the limit supported by a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

81.38 tmnxVdoVappSGLimitExceeded

Table 1888: tmnxVdoVappSGLimitExceeded properties

Property name	Value
Application name	VIDEO
Event ID	2024
Event name	tmnxVdoVappSGLimitExceeded
SNMP notification prefix and OID	TIMETRA-VIDEO-MIB.tmnxVdoNotifications.24
Default severity	warning
Source stream	main
Message format string	Threshold for number of channels exceeded - *$tmnxVdoGrpVapp Channels$* channels active on VAPP *$tmnxVdoGrpEsaNum$*/*$tmnx VdoGrpEsaVappNum$*, video group - *$tmnxVdoGrpId$*
Cause	A tmnxVdoVappSGLimitExceeded notification is generated when the configuration exceeds the maximum number of channels supported by a video Media Dependent Adapter (MDA).
Effect	N/A
Recovery	N/A

82 VRRP

82.1 tmnxVrrpBecameBackup

Table 1889: 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
Source stream	main
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

82.2 tmnxVrrpBfdIntfSessStateChgd

Table 1890: tmnxVrrpBfdIntfSessStateChgd properties

Property name	Value
Application name	VRRP
Event ID	2008
Event name	tmnxVrrpBfdIntfSessStateChgd
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.5

Property name	Value
Default severity	minor
Source stream	main
Message format string	BFD session on service *$tmnxVrrpNotifBfdIntfSvcId$* interface *$tmnx VrrpNotifBfdIntfIfName$* to peer *$tmnxVrrpNotifBfdIntfDestIp$* changed state to *$tmnxVrrpNotifBfdIntfSessState$*.
Cause	The operational state of a BFD session of the VRRP instance changed.
Effect	N/A
Recovery	N/A

82.3 tmnxVrrpIPListMismatch

Table 1891: 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
Source stream	main
Message format string	IP Address list in VRRP advertisement from *$tmnxVrrpRouterMaster PrimaryAddr$* 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

82.4 tmnxVrrpIPListMismatchClear

Table 1892: tmnxVrrpIPListMismatchClear properties

Property name	Value
Application name	VRRP
Event ID	2004
Event name	tmnxVrrpIPListMismatchClear
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.2
Default severity	minor
Source stream	main
Message format string	Previously generated address list mismatch trap cleared for VRRP instance *$vrrpOperVrId$* on interface *$ifIndex$* for advertisements from *$tmnxVrrpRouterMasterPrimaryAddr$*
Cause	A previously occurring 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

82.5 tmnxVrrpMultipleOwners

Table 1893: tmnxVrrpMultipleOwners properties

Property name	Value
Application name	VRRP
Event ID	2005
Event name	tmnxVrrpMultipleOwners
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.3

Property name	Value
Default severity	minor
Source stream	main
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

82.6 tmnxVrrpOperDownInvalidMac

Table 1894: 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
Source stream	main
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."

82.7 tmnxVrrpOperDownInvalidMacClear

Table 1895: 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
Source stream	main
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 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."

82.8 tVrrpBecameBackup

Table 1896: tVrrpBecameBackup properties

Property name	Value
Application name	VRRP
Event ID	2010
Event name	tVrrpBecameBackup
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.6

Property name	Value
Default severity	minor
Source stream	main
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

82.9 tVrrpIPListMismatch

Table 1897: tVrrpIPListMismatch properties

Property name	Value
Application name	VRRP
Event ID	2012
Event name	tVrrpIPListMismatch
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.8
Default severity	minor
Source stream	main
Message format string	IPv6 Address list in VRRP advertisement from *$tVrrpRtrMasterPrimary Addr$* did not match address list configured for VRRP instance *$vrrp OperationsVrId$* 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

82.10 tVrrpIPListMismatchClear

Table 1898: 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
Source stream	main
Message format string	Previously generated address list mismatch trap cleared for VRRP instance *$vrrpOperationsVrId$* on interface *$ifIndex$* for advertisements from *$tVrrpRtrMasterPrimaryAddr$*
Cause	A previously occurring 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

82.11 tVrrpMultipleOwners

Table 1899: tVrrpMultipleOwners properties

Property name	Value
Application name	VRRP
Event ID	2014
Event name	tVrrpMultipleOwners
SNMP notification prefix and OID	TIMETRA-VRRP-MIB.tmnxVrrpNotifications.10

Property name	Value
Default severity	minor
Source stream	main
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

82.12 tVrrpOperDownInvalidMac

Table 1900: 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
Source stream	main
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.
Effect	The VRRP virtual router instance is not allowed to become operationally 'up'.
Recovery	There is no recovery required for this notification."

82.13 tVrrpOperDownInvalidMacClear

Table 1901: 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
Source stream	main
Message format string	tVrrpOperDownInvalidMac notification from IPv6 VR *$vrrpOperations VrId$* 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."

82.14 tVrrpPacketDiscarded

Table 1902: tVrrpPacketDiscarded properties

Property name	Value
Application name	VRRP
Event ID	2015
Event name	tVrrpPacketDiscarded
SNMP notification prefix and OID	N/A

Property name	Value
Default severity	minor
Source stream	main
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

82.15 tVrrpRouterAdvNotActivated

Table 1903: 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
Source stream	main
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

82.16 tVrrpRouterAdvNotActivatedClear

Table 1904: 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
Source stream	main
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

82.17 tVrrpTrapNewMaster

Table 1905: 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

Property name	Value
Source stream	main
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
Recovery	N/A

82.18 vrrpPacketDiscarded

Table 1906: vrrpPacketDiscarded properties

Property name	Value
Application name	VRRP
Event ID	2007
Event name	vrrpPacketDiscarded
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
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

82.19 vrrpTrapAuthFailure

Table 1907: 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
Source stream	main
Message format string	Authentication failed for VRRP packet received from *$vrrpTrapPacketSrc$* 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

82.20 vrrpTrapNewMaster

Table 1908: 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
Source stream	main

Property name	Value
Message format string	VRRP virtual router instance *$vrrpOperVrId$* on interface *$ifIndex$* (primary address *$vrrpOperMasterIpAddr$*) changed state to master
Cause	The sending agent has transitioned to 'Master' state.
Effect	N/A
Recovery	N/A

82.21 vrrpTrapProtoError

Table 1909: vrrpTrapProtoError properties

Property name	Value
Application name	VRRP
Event ID	2009
Event name	vrrpTrapProtoError
SNMP notification prefix and OID	VRRP-MIB.vrrpNotifications.3
Default severity	minor
Source stream	main
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

83 VRTR

83.1 tipNbrAllocFailed

Table 1910: tipNbrAllocFailed properties

Property name	Value
Application name	VRTR
Event ID	2095
Event name	tipNbrAllocFailed
SNMP notification prefix and OID	N/A
Default severity	minor
Source stream	main
Message format string	Not enough memory to allocate neighbor *$neighbor$* on itf *$interface$*
Cause	Either unable to allocate memory for the neighbor or unable to allocate hardware resources.
Effect	Cannot create a new IPv6 neighbor structure.
Recovery	N/A

83.2 tmnxVRtrArpLmt

Table 1911: tmnxVRtrArpLmt properties

Property name	Value
Application name	VRTR
Event ID	2077
Event name	tmnxVRtrArpLmt
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.77

Property name	Value
Default severity	minor
Source stream	main
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.

83.3 tmnxVRtrArpThresholdExceeded

Table 1912: 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
Source stream	main
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.

Property name	Value
Recovery	Increase the arp-limit.

83.4 tmnxVRtrBfdExtNoCpmNpResources

Table 1913: 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
Source stream	main
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 or fp session termination resource (see vRtrIfBfdExt Type), and no cpmNp or fp session termination resources are available.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

83.5 tmnxVRtrBfdExtNoFreeTxIntrvlSlot

Table 1914: tmnxVRtrBfdExtNoFreeTxIntrvlSlot properties

Property name	Value
Application name	VRTR
Event ID	2098

Property name	Value
Event name	tmnxVRtrBfdExtNoFreeTxIntrvlSlot
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.98
Default severity	minor
Source stream	main
Message format string	The BFD session of type fp with local discriminator *$vRtrIfBfdSessExt LclDisc$* on node *$subject$* must use another transmit interval than negotiated with the peer because all transmit interval slots available in hardware (8) are already in use
Cause	The tmnxVRtrBfdExtNoFreeTxIntrvlSlot is generated when a BFD session of type fp must use another transmit interval than negotiated with the peer because all transmit interval slots available in hardware (8) are already in use.
Effect	There is no effect of this notification.
Recovery	The problem can be mitigated by changing the configuration on this node and its peer nodes to use maximum 8 combinations of local multiplier, local transmit interval and remote receive interval.

83.6 tmnxVRtrBfdMaxSessionOnSlot

Table 1915: 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
Source stream	main
Message format string	The number of *$vRtrBfdAllocateGroup$* BFD sessions on *$vRtrSlot OrCpmFlag$ $vRtrBfdSlotNumber$* has exceeded the limit of *$vRtr NumberOfBfdSessionsOnSlot$* sessions, constrained by *$vRtrBfdMax SessionReason$*.

Property name	Value
Cause	The tmnxVRtrBfdMaxSessionOnSlot notification is generated for several reasons, indicated by vRtrBfdMaxSessionReason. When 'max SessionsPerSlot' the maximum number of BFD sessions indicated by vRtrNumberOfBfdSessionsOnSlot has been reached, when 'max TxPacketRate' or 'maxRxPacketRate' then the maximum transmit or receive packet rate limit is exceeded, indicated by vRtrAllocatedBfd TxPacketRate or vRtrAllocatedBfdRxPacketRate. The location where the limit has been reached is indicated by vRtrSlotOrCpmFlag. vRtr BfdSlotNumber indicates the slot when vRtrSlotOrCpmFlag is 'slot' or 'xcm'. For CPM based sessions vRtrSlotOrCpmFlag will have the value 'cpm'. The maximum number of table entries available on the slot is indicated by vRtrBfdMaxTableEntries, when 'maxTableEntries'.
Effect	N/A
Recovery	N/A

83.7 tmnxVRtrBfdMultiHopFpMismatch

Table 1916: tmnxVRtrBfdMultiHopFpMismatch properties

Property name	Value
Application name	VRTR
Event ID	2100
Event name	tmnxVRtrBfdMultiHopFpMismatch
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.100
Default severity	warning
Source stream	main
Message format string	The multi-hop BFD session with local discriminator *$vRtrIfBfdSessExt LclDisc$* on interface *$vRtrIfIndex$* (local *$vRtrIfBfdSessExtLclAddr$*, remote *$vRtrIfBfdSessExtRemAddr$*) will go down if peer packets do not arrive on slot *$vRtrBfdSlotNumber$*, FP *$vRtrNotifyFpNum$*
Cause	The tmnxVRtrBfdMultiHopFpMismatch is generated on certain platforms when a BFD session is created where: - the stream of the BFD packets that this system transmits could change from one FP to another, or - this system could receive the BFD packets on another FP than the one that transmits them.

Property name	Value
Effect	BFD packets could be dropped and the BFD session could report a loss.
Recovery	Design the network such that this system always transmits and receives the streams of packets for any given BFD session using the same FP.

83.8 tmnxVRtrBfdPortTypeNotSupported

Table 1917: 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
Source stream	main
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

83.9 tmnxVRtrBfdSessExtDeleted

Table 1918: tmnxVRtrBfdSessExtDeleted properties

Property name	Value
Application name	VRTR
Event ID	2063

Property name	Value
Event name	tmnxVRtrBfdSessExtDeleted
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.63
Default severity	minor
Source stream	main
Message format string	BFD Session on node *$subject$* has been deleted.
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.

83.10 tmnxVRtrBfdSessExtDown

Table 1919: 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
Source stream	main
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.

83.11 tmnxVRtrBfdSessExtProtChange

Table 1920: tmnxVRtrBfdSessExtProtChange properties

Property name	Value
Application name	VRTR
Event ID	2064
Event name	tmnxVRtrBfdSessExtProtChange
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.64
Default severity	minor
Source stream	main
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.

83.12 tmnxVRtrBfdSessExtUp

Table 1921: 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
Source stream	main

Property name	Value
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.

83.13 tmnxVRtrDhcp6ClientStatusChanged

Table 1922: tmnxVRtrDhcp6ClientStatusChanged properties

Property name	Value
Application name	VRTR
Event ID	2087
Event name	tmnxVRtrDhcp6ClientStatusChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.87
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$*: DHCPv6 client status changed to *$vRtr IfDhcp6ClStateStatus$ - $vRtrIfDhcp6ClStateDescription$*
Cause	The tmnxVRtrDhcp6ClientStatusChanged notification is sent when the value of the object vRtrIfDhcp6ClStateStatus changes.
Effect	While the value of the object vRtrIfDhcp6ClStateDescription is not equal to 'established', the DHCP client is not operational.
Recovery	The recovery action, if necessary, depends on the actual state. When the value is 'failed', details about the failure cause are specified in the v RtrIfDhcp6ClStateDescription.

83.14 tmnxVRtrDhcpClientStatusChanged

Table 1923: tmnxVRtrDhcpClientStatusChanged properties

Property name	Value
Application name	VRTR
Event ID	2086
Event name	tmnxVRtrDhcpClientStatusChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.86
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$*: DHCP client status changed to *$vRtrIfDhcp ClStateStatus$ - $vRtrIfDhcpClStateDescription$*
Cause	The tmnxVRtrDhcpClientStatusChanged notification is sent when the value of the object vRtrIfDhcpClStateStatus changes.
Effect	While the value of the object vRtrIfDhcpClStateDescription is not equal to 'established', the DHCP client is not operational.
Recovery	The recovery action, if necessary, depends on the actual state. When the value is 'failed', details about the failure cause are specified in the v RtrIfDhcpClStateDescription.

83.15 tmnxVRtrDnsFault

Table 1924: tmnxVRtrDnsFault properties

Property name	Value
Application name	VRTR
Event ID	2066
Event name	tmnxVRtrDnsFault
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.66
Default severity	minor
Source stream	main
Message format string	Fault with DNS server *$vRtrNotifInetAddr$ $vRtrNotifTruthValue$ - $v RtrFailureDescription$*

Property name	Value
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.

83.16 tmnxVRtrFibOccupancyThreshold

Table 1925: 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
Source stream	main
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

83.17 tmnxVRtrFibVPNOccupancyThreshold

Table 1926: tmnxVRtrFibVPNOccupancyThreshold properties

Property name	Value
Application name	VRTR
Event ID	2099
Event name	tmnxVRtrFibVPNOccupancyThreshold
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.99
Default severity	minor
Source stream	main
Message format string	High VPN FIB utilization detected.
Cause	The VPN FIB on an IOM card transitioned between experiencing persistent normal and high utilization.
Effect	N/A
Recovery	N/A

83.18 tmnxVRtrGrtExportLimitReached

Table 1927: 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
Source stream	main
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.

Property name	Value
Recovery	Change GRT export policy.

83.19 tmnxVRtrGrtRoutesExpLimitDropped

Table 1928: 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
Source stream	main
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

83.20 tmnxVRtrGrtV6ExportLimitReached

Table 1929: tmnxVRtrGrtV6ExportLimitReached properties

Property name	Value
Application name	VRTR
Event ID	2032
Event name	tmnxVRtrGrtV6ExportLimitReached
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.44

Property name	Value
Default severity	major
Source stream	main
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.

83.21 tmnxVRtrGrtV6RoutesExpLimDropped

Table 1930: 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
Source stream	main
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
Recovery	N/A

83.22 tmnxVRtrHighRouteCleared

Table 1931: 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
Source stream	main
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

83.23 tmnxVRtrHighRouteTCA

Table 1932: 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
Source stream	main
Message format string	Router *$subject$* has exceeded the high-level threshold: *$vRtrHigh RouteThreshold$* - the routing table contains *$vRtrStatCurrNumRoutes $* routes
Cause	The high-level threshold for number of routes has been crossed.

Property name	Value
Effect	N/A
Recovery	N/A

83.24 tmnxVRtrIfIgnorePortState

Table 1933: 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
Source stream	main
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."

83.25 tmnxVRtrIfLdpSyncTimerStart

Table 1934: tmnxVRtrIfLdpSyncTimerStart properties

Property name	Value
Application name	VRTR
Event ID	2029

Property name	Value
Event name	tmnxVRtrIfLdpSyncTimerStart
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.41
Default severity	warning
Source stream	main
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

83.26 tmnxVRtrIfLdpSyncTimerStop

Table 1935: 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
Source stream	main
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

83.27 tmnxVRtrInetAddressAttachFailed

Table 1936: tmnxVRtrInetAddressAttachFailed properties

Property name	Value
Application name	VRTR
Event ID	2024
Event name	tmnxVRtrInetAddressAttachFailed
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.37
Default severity	minor
Source stream	main
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

83.28 tmnxVRtrIPv6HighRouteCleared

Table 1937: 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
Source stream	main

Property name	Value
Message format string	Router *$subject$* has cleared the high-level threshold: *$vRtrIPv6High RouteThreshold$* - the routing table contains *$vRtrV6StatCurrNum Routes$* IPv6 routes
Cause	The number of IPv6 routes has dropped below the high-level threshold.
Effect	N/A
Recovery	N/A

83.29 tmnxVRtrIPv6HighRouteTCA

Table 1938: 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
Source stream	main
Message format string	Router *$subject$* has exceeded the high-level threshold: *$v RtrIPv6HighRouteThreshold$* - the routing table contains *$vRtrV6Stat CurrNumRoutes$* IPv6 routes
Cause	The high-level threshold for number of IPv6 routes has been crossed.
Effect	N/A
Recovery	N/A

83.30 tmnxVRtrIPv6MidRouteTCA

Table 1939: 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
Source stream	main
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

83.31 tmnxVRtrIpv6NbrLmt

Table 1940: 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
Source stream	main
Message format string	Interface *$vRtrIfName$*: Number of neighbor entries learned has exceeded the configured maximum (*$vRtrIfIpv6NbrLimit$*)

Property name	Value
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.

83.32 tmnxVRtrIpv6NbrThresholdExceeded

Table 1941: 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
Source stream	main
Message format string	Interface *$vRtrIfName$*: Number of neighbor entries learned has exceeded the *$vRtrIfIpv6NbrThreshold$* percentage of the configured maximum (*$vRtrIfIpv6NbrLimit$*)
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.

83.33 tmnxVRtrLeakExportLimitDropped

Table 1942: tmnxVRtrLeakExportLimitDropped properties

Property name	Value
Application name	VRTR
Event ID	2085
Event name	tmnxVRtrLeakExportLimitDropped
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.85
Default severity	minor
Source stream	main
Message format string	The number of routes exported from the GRT has dropped below the export limit *$vRtrLeakExportLimit$*
Cause	The tmnxVRtrLeakExportLimitDropped notification is generated when the number of leaked routes drops below the leak-export-limit.
Effect	Some routes allowed by the leak-export policies may not have been leaked to the target VPRNs.
Recovery	Not applicable.

83.34 tmnxVRtrLeakExportLimitReached

Table 1943: tmnxVRtrLeakExportLimitReached properties

Property name	Value
Application name	VRTR
Event ID	2084
Event name	tmnxVRtrLeakExportLimitReached
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.84
Default severity	minor
Source stream	main

Property name	Value
Message format string	GRT has reached the export-limit *$vRtrLeakExportLimit$*, additional routes will not be exported into VPRN
Cause	The tmnxVRtrLeakExportLimitReached notification is generated when the leak-export-limit has been exceeded.
Effect	Some routes allowed by the leak-export policies may not have been leaked to the target VPRNs.
Recovery	Not applicable.

83.35 tmnxVRtrMacAcctLimitCleared

Table 1944: 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
Source stream	main
Message format string	Mac Accounting Indices are available for RtrId *$vRtrID$* Interface *$vRtrIfName$*
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.

83.36 tmnxVRtrMacAcctLimitReached

Table 1945: 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
Source stream	main
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.

83.37 tmnxVRtrManagedRouteAddFailed

Table 1946: 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
Source stream	main

Property name	Value
Message format string	Could not install managed route *$vRtrManagedRouteInetAddr$*/ *$vRtr ManagedRoutePrefixLen$* in router *$subject$* : *$vRtrFailureDescription $*
Cause	A managed route could not be installed.
Effect	N/A
Recovery	N/A

83.38 tmnxVRtrMaxArpEntriesCleared

Table 1947: 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
Source stream	main
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

83.39 tmnxVRtrMaxArpEntriesTCA

Table 1948: 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
Source stream	main
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

83.40 tmnxVRtrMaxRoutes

Table 1949: 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
Source stream	main
Message format string	Router *$subject$* has exceeded the max *$vRtrMaxRoutesType$* routes threshold: *$vRtrMaxNumRoutes$* - the VRF contains *$vRtrStatCurr NumRoutes$* routes

Property name	Value
Cause	The maximum routes threshold contained in a VPRN has been crossed.
Effect	N/A
Recovery	N/A

83.41 tmnxVRtrMcastMaxRoutesCleared

Table 1950: tmnxVRtrMcastMaxRoutesCleared properties

Property name	Value
Application name	VRTR
Event ID	2007
Event name	tmnxVRtrMcastMaxRoutesCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.7
Default severity	minor
Source stream	main
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

83.42 tmnxVRtrMcastMaxRoutesTCA

Table 1951: tmnxVRtrMcastMaxRoutesTCA properties

Property name	Value
Application name	VRTR

Property name	Value
Event ID	2006
Event name	tmnxVRtrMcastMaxRoutesTCA
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.6
Default severity	minor
Source stream	main
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

83.43 tmnxVRtrMcastMidRouteTCA

Table 1952: 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
Source stream	main
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

Property name	Value
Recovery	N/A

83.44 tmnxVRtrMidRouteTCA

Table 1953: 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
Source stream	main
Message format string	Router *$subject$* has exceeded the mid-level threshold: *$vRtrMidRouteThreshold$* - the routing table contains *$vRtrStatCurrNumRoutes$* routes
Cause	The mid-level threshold for number of routes has been crossed.
Effect	N/A
Recovery	N/A

83.45 tmnxVRtrNeDiscovered

Table 1954: tmnxVRtrNeDiscovered properties

Property name	Value
Application name	VRTR
Event ID	2088
Event name	tmnxVRtrNeDiscovered
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.88

Property name	Value
Default severity	warning
Source stream	main
Message format string	Possible messages: • New NE discovered: RtrId *$vRtrID$*, NEID 0x*$tmnxVRtrNeInfo Neid$*, NEIP (ipv4 *$tmnxVRtrNeInfoNeipV4$*/*$tmnxVRtrNeInfo NeipV4PrefixLen$*, ipv6 N.A.), system-mac *$tmnxVRtrNeInfo SystemMac$*, vendor-id *$tmnxVRtrNeInfoVendorId$*, platform-type *$tmnxVRtrNeInfoPlatformType$* • New NE discovered: RtrId *$vRtrID$*, NEID 0x*$tmnxVRtrNeInfo Neid$*, NEIP (ipv4 *$tmnxVRtrNeInfoNeipV4$*/ *$tmnxVRtrNeInfo NeipV4PrefixLen$*, ipv6 *$tmnxVRtrNeInfoNeipV6$*/*$tmnxVRtrNeInfo NeipV6PrefixLen$*), system-mac *$tmnxVRtrNeInfoSystemMac$*, vendor-id *$tmnxVRtrNeInfoVendorId$*, platform-type *$tmnxVRtr NeInfoPlatformType$*
Cause	The tmnxVRtrNeDiscovered notification is sent when a new Network Element is discovered.
Effect	No effect.
Recovery	No recovery is necessary.

83.46 tmnxVRtrNeModified

Table 1955: tmnxVRtrNeModified properties

Property name	Value
Application name	VRTR
Event ID	2090
Event name	tmnxVRtrNeModified
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.90
Default severity	warning
Source stream	main
Message format string	Possible messages: • NE modified: RtrId *$vRtrID$*, NEID 0x*$tmnxVRtrNeInfoNeid$*, NEIP (ipv4 *$tmnxVRtrNeInfoNeipV4$*/ *$tmnxVRtrNeInfoNeipV4PrefixLen $*, ipv6 N.A.), system-mac *$tmnxVRtrNeInfoSystemMac$*, vendor-

Property name	Value
	id *$tmnxVRtrNeInfoVendorId$*, platform-type *$tmnxVRtrNeInfo PlatformType$* • NE modified: RtrId *$vRtrID$*, NEID 0x*$tmnxVRtrNeInfoNeid$*, NEIP (ipv4 *$tmnxVRtrNeInfoNeipV4$*/*$tmnxVRtrNeInfoNeipV4PrefixLen$*, ipv6 *$tmnxVRtrNeInfoNeipV6$*/*$tmnxVRtrNeInfoNeipV6PrefixLen$*), system-mac *$tmnxVRtrNeInfoSystemMac$*, vendor-id *$tmnxVRtr NeInfoVendorId$*, platform-type *$tmnxVRtrNeInfoPlatformType$*
Cause	The tmnxVRtrNeModified notification is sent when a Network Element is modified.
Effect	No effect.
Recovery	No recovery is necessary.

83.47 tmnxVRtrNeRemoved

Table 1956: tmnxVRtrNeRemoved properties

Property name	Value
Application name	VRTR
Event ID	2089
Event name	tmnxVRtrNeRemoved
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.89
Default severity	warning
Source stream	main
Message format string	Possible messages: • NE removed: RtrId *$vRtrID$*, NEID 0x*$tmnxVRtrNeInfoNeid$*, NEIP (ipv4 *$tmnxVRtrNeInfoNeipV4$*/ *$tmnxVRtrNeInfoNeipV4PrefixLen $*, ipv6 N.A.), system-mac *$tmnxVRtrNeInfoSystemMac$*, vendor-id *$tmnxVRtrNeInfoVendorId$*, platform-type *$tmnxVRtrNeInfo PlatformType$* • NE removed: RtrId *$vRtrID$*, NEID 0x*$tmnxVRtrNeInfoNeid$*, NEIP (ipv4 *$tmnxVRtrNeInfoNeipV4$*/*$tmnxVRtrNeInfoNeipV4PrefixLen$*, ipv6 *$tmnxVRtrNeInfoNeipV6$*/*$tmnxVRtrNeInfoNeipV6PrefixLen$*), system-mac *$tmnxVRtrNeInfoSystemMac$*, vendor-id *$tmnxVRtr NeInfoVendorId$*, platform-type *$tmnxVRtrNeInfoPlatformType$*

Property name	Value
Cause	The tmnxVRtrNeRemoved notification is sent when a Network Element is removed.
Effect	No effect.
Recovery	No recovery is necessary.

83.48 tmnxVRtrNgBfdNoCpmNpResources

Table 1957: 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
Source stream	main
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 or fp session termination resource (see vRtrIfBfdExt Type), and no cpmNp or fp session termination resources are available.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

83.49 tmnxVRtrNgBfdSessDeleted

Table 1958: 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
Source stream	main
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.
Effect	There is no effect of this notification.
Recovery	There is no recovery required for this notification.

83.50 tmnxVRtrNgBfdSessDown

Table 1959: 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
Source stream	main
Message format string	*$vRtrIfBfdSessExtLinkType$* BFD session with Local Discriminator *$vRtrIfBfdSessExtLclDisc$* on *$subject$* is down due to *$vRtrIfBfdSessExtOperFlags$*

Property name	Value
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 its own.

83.51 tmnxVRtrNgBfdSessProtChange

Table 1960: tmnxVRtrNgBfdSessProtChange properties

Property name	Value
Application name	VRTR
Event ID	2072
Event name	tmnxVRtrNgBfdSessProtChange
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.72
Default severity	minor
Source stream	main
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.

83.52 tmnxVRtrNgBfdSessUp

Table 1961: 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
Source stream	main
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.

83.53 tmnxVRtrNHRvplsARPExhaust

Table 1962: tmnxVRtrNHRvplsARPExhaust properties

Property name	Value
Application name	VRTR
Event ID	2075
Event name	tmnxVRtrNHRvplsARPExhaust
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.75
Default severity	minor
Source stream	main
Message format string	The Next Hop RVPLS ARP entries reached 100 percent of its limit *$tmnxVRtrMaxNHRvplsARPEntries$*

Property name	Value
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.

83.54 tmnxVRtrNHRvplsARPHighUsage

Table 1963: 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
Source stream	main
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.

83.55 tmnxVRtrNHRvplsARPHighUsageClr

Table 1964: 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
Source stream	main
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.

83.56 tmnxVRtrPdnAddrMismatch

Table 1965: tmnxVRtrPdnAddrMismatch properties

Property name	Value
Application name	VRTR
Event ID	2082
Event name	tmnxVRtrPdnAddrMismatch
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.82
Default severity	minor
Source stream	main
Message format string	RtrId *$vRtrID$* PDN interface *$vRtrIfName$* PDN IP address *$vRtrNotifInetAddr$* mismatch - *$vRtrFailureDescription$*

Property name	Value
Cause	The tmnxVRtrPdnAddrMismatch notification is generated when the IP address learned by the PDN interface through the cellular network could not be installed on the PDN router interface. For IPv4, this occurs when the parent interface has a mismatching configured IP address or when the learned PDN IP address overlaps another IP address in the router instance. The notification will only be generated when the PDN interface is set unnumbered to the system interface or any other existing loopback interface. For IPv6 operation, this occurs when the IPv6 address has a mismatching subnet to the address configured for the PDN router interface or if the exact same IPv6 address is configured on the PDN interface as the address received by the network.
Effect	The PDN Interface will be operationally down.
Recovery	Check the configured IP address for the PDN interface or parent interface, check the other IP addresses in the router instance, and/or check the state of the cellular network.

83.57 tmnxVRtrPdnAddrMismatchCleared

Table 1966: tmnxVRtrPdnAddrMismatchCleared properties

Property name	Value
Application name	VRTR
Event ID	2083
Event name	tmnxVRtrPdnAddrMismatchCleared
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.83
Default severity	minor
Source stream	main
Message format string	RtrId *$vRtrID$* PDN interface *$vRtrIfName$* PDN IP address mismatch cleared
Cause	The tmnxVRtrPdnAddrMismatchCleared notification is generated when the conditions that caused the PDN address mismatch no longer exist.
Effect	The PDN interface will go operationally up.
Recovery	Not applicable.

83.58 tmnxVRtrSingleSfmOverloadStateCh

Table 1967: 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
Source stream	main
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 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.

83.59 tmnxVRtrStaticRouteCPEStatus

Table 1968: 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

Property name	Value
Source stream	main
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

83.60 tmnxVRtrStaticRouteStatusChanged

Table 1969: 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
Source stream	main
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

83.61 vRtrAutoCfgRaRtStatusChanged

Table 1970: vRtrAutoCfgRaRtStatusChanged properties

Property name	Value
Application name	VRTR
Event ID	2093
Event name	vRtrAutoCfgRaRtStatusChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.93
Default severity	minor
Source stream	main
Message format string	NDP RA route *$vRtrAutoCfgRaRtAddr$*/*$vRtrAutoCfgRaRtPrefixLen$* next-hop *$vRtrAutoCfgRaRtNhAddr$* status changed to *$vRtrAutoCfg RaRtStatus$*
Cause	The vRtrAutoCfgRaRtStatusChanged notification is sent when the value of the object vRtrAutoCfgRaRtStatus changes; that includes when a row in the vRtrAutoCfgRaRtTable is created or destroyed.
Effect	A value of 'installed' indicates the received route is valid, and is successfully installed in the route table.
Recovery	The recovery action, if necessary, depends on the actual state.

83.62 vRtrBgpInstanceError

Table 1971: vRtrBgpInstanceError properties

Property name	Value
Application name	VRTR
Event ID	2101
Event name	vRtrBgpInstanceError
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.101
Default severity	minor

Property name	Value
Source stream	main
Message format string	Virtual router *$vRtrID$* BGP type *$vRtrNotifyBgpInstType$* and instance *$vRtrNotifyBgpInstance$* had error: *$vRtrFailureDescription$*
Cause	The vRtrBgpInstanceError is generated on certain platforms when BGP instance generates an error.
Effect	Associated BGP instance may be operationally down.
Recovery	Design the network such that this system uses resources properly.

83.63 vRtrIfDhcp6ClStateDnsChanged

Table 1972: vRtrIfDhcp6ClStateDnsChanged properties

Property name	Value
Application name	VRTR
Event ID	2094
Event name	vRtrIfDhcp6ClStateDnsChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.94
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$*: DHCP6 client DNS addresses changed to DNS1= *$vRtrIfDhcp6ClStateDnsPriAddr$* DNS2=*$vRtrIfDhcp6ClStateDnsSecAddr$* DNS3=*$vRtrIfDhcp6ClStateDnsTerAddr$*
Cause	The vRtrIfDhcp6ClStateDnsChanged notification is sent when the value of any of the DNS addresses of the DHCP6 client changes.
Effect	[RECOVERY]
Recovery	N/A

83.64 vRtrIfDhcpClRtStatusChanged

Table 1973: vRtrIfDhcpClRtStatusChanged properties

Property name	Value
Application name	VRTR
Event ID	2091
Event name	vRtrIfDhcpClRtStatusChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.91
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$*: DHCP client route *$vRtrIfDhcpClRtAddr$*/*$vRtrIfDhcpClRtPrefixLen$* next-hop *$vRtrIfDhcpClRtNhAddr$* status changed to *$vRtrIfDhcpClRtStatus$*
Cause	The vRtrIfDhcpClRtStatusChanged notification is sent when the value of the object vRtrIfDhcpClRtStatus changes; that includes when a row in the vRtrIfDhcpClRtTable is created or destroyed.
Effect	A value of 'installed' indicates the received route is valid, and is successfully installed in the route table.
Recovery	The recovery action, if necessary, depends on the actual state.

83.65 vRtrIfDhcpClStateDnsChanged

Table 1974: vRtrIfDhcpClStateDnsChanged properties

Property name	Value
Application name	VRTR
Event ID	2092
Event name	vRtrIfDhcpClStateDnsChanged
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.92
Default severity	minor
Source stream	main

Property name	Value
Message format string	Interface *$vRtrIfIndex$*: DHCP client DNS addresses changed to DNS1= *$vRtrIfDhcpClStateDnsPriAddr$* DNS2=*$vRtrIfDhcpClStateDnsSecAddr$* DNS3=*$vRtrIfDhcpClStateDnsTerAddr$*
Cause	The vRtrIfDhcpClStateDnsChanged notification is sent when the value of any of the DNS addresses of the DHCP client changes.
Effect	[RECOVERY]
Recovery	N/A

83.66 vRtrIfEthLoopbackStarted

Table 1975: vRtrIfEthLoopbackStarted properties

Property name	Value
Application name	VRTR
Event ID	2096
Event name	vRtrIfEthLoopbackStarted
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.96
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$*: Loopback started.
Cause	The vRtrIfEthLoopbackStarted notification is generated when the router interface is placed into loopback.
Effect	None
Recovery	N/A

83.67 vRtrIfEthLoopbackStopped

Table 1976: vRtrIfEthLoopbackStopped properties

Property name	Value
Application name	VRTR
Event ID	2097
Event name	vRtrIfEthLoopbackStopped
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.97
Default severity	minor
Source stream	main
Message format string	Interface *$vRtrIfIndex$*: Loopback stopped.
Cause	The vRtrIfEthLoopbackStopped notification is generated when the router interface is removed from loopback.
Effect	None
Recovery	N/A

83.68 vrtrIfIpTunnelOperStateChange

Table 1977: vrtrIfIpTunnelOperStateChange properties

Property name	Value
Application name	VRTR
Event ID	2102
Event name	vrtrIfIpTunnelOperStateChange
SNMP notification prefix and OID	TIMETRA-VRTR-MIB.tmnxVRtrNotifications.102
Default severity	minor
Source stream	main
Message format string	Operational state change for IP Tunnel *$vRtrIfIpTunnelName$* on interface *$vRtrIfIndex$*, admin state: *$vRtrIfIpTunnelAdminState$*, oper state: *$vRtrIfIpTunnelOperState$*, oper flags: *$vRtrIfIpTunnelOperFlags$*

Property name	Value
Cause	The vrtrIfIpTunnelOperStateChange notification is generated when there is a change in state 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

84 WLAN_GW

84.1 tmnxWlanGwBdCreated

Table 1978: tmnxWlanGwBdCreated properties

Property name	Value
Application name	WLAN_GW
Event ID	2022
Event name	tmnxWlanGwBdCreated
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.26
Default severity	minor
Source stream	main
Message format string	The WLAN Gateway Bridge Domain with identifier *$tmnxWlanGwNotifyBdBridgeId$* has been created in the system.
Cause	The system issues the tmnxWlanGwBdCreated notification when it creates a conceptual row in the tmnxWlanGwBdTable.
Effect	The system is aware of a WLAN Gateway Bridge Domain and has context for it.
Recovery	Not required. This notification is informational.

84.2 tmnxWlanGwBdDeleted

Table 1979: tmnxWlanGwBdDeleted properties

Property name	Value
Application name	WLAN_GW
Event ID	2023
Event name	tmnxWlanGwBdDeleted

Property name	Value
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.27
Default severity	minor
Source stream	main
Message format string	The WLAN Gateway Bridge Domain with identifier *$tmnxWlanGwNotifyBdBridgeId$* has been removed from the system.
Cause	The system issues the tmnxWlanGwBdDeleted notification when it destroys a conceptual row in the tmnxWlanGwBdTable.
Effect	The system has become unaware of a WLAN Gateway Bridge Domain.
Recovery	Recovery may or may not be required, depending of the cause.

84.3 tmnxWlanGwDsmGtpTunnelSetupFail

Table 1980: 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
Source stream	main
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.

84.4 tmnxWlanGwGrpMemberUsageHigh

Table 1981: tmnxWlanGwGrpMemberUsageHigh properties

Property name	Value
Application name	WLAN_GW
Event ID	2026
Event name	tmnxWlanGwGrpMemberUsageHigh
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.30
Default severity	warning
Source stream	main
Message format string	The *$tmnxWlanGwNotifyEntity$* usage high water status changed to *$tmnxWlanGwNotifyTrue$* on ISA group *$tmnxWlanGwNotifyIsaGrpId$* member *$tmnxWlanGwNotifyIsaMemberId$* on *$tmnxWlanGwNotifyChassisIndex$*/*$tmnxWlanGwNotifyCardSlotNum$*/*$tmnxWlanGwNotifyMdaSlotNum$*. (EsaNum *$tmnxWlanGwNotifyEsaNum$*, EsaVappNum *$tmnxWlanGwNotifyEsaVappNum$*)
Cause	The tmnxWlanGwGrpMemberUsageHigh notification is sent when the usage of a particular entity on a WLAN Gateway ISA group member reaches its high watermark ('true') or when it reaches its low watermark again ('false').
Effect	N/A
Recovery	N/A

84.5 tmnxWlanGwGrpOperStateChanged

Table 1982: tmnxWlanGwGrpOperStateChanged properties

Property name	Value
Application name	WLAN_GW
Event ID	2004
Event name	tmnxWlanGwGrpOperStateChanged

Property name	Value
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.4
Default severity	minor
Source stream	main
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

84.6 tmnxWlanGwGtpMessageDropped

Table 1983: 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
Source stream	main
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.

84.7 tmnxWlanGwIomActive

Table 1984: 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
Source stream	main
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

84.8 tmnxWlanGwMgwConnected

Table 1985: 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

Property name	Value
Source stream	main
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.
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.

84.9 tmnxWlanGwMgwRestarted

Table 1986: 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
Source stream	main
Message format string	The Mobile Gateway has restarted. The restart count is *$tmnxWlanGwMgwRestartCount$*.
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).

Property name	Value
Recovery	No recovery is required on this system.

84.10 tmnxWlanGwMgwStateChanged

Table 1987: tmnxWlanGwMgwStateChanged properties

Property name	Value
Application name	WLAN_GW
Event ID	2009
Event name	tmnxWlanGwMgwStateChanged
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.13
Default severity	minor
Source stream	main
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.

84.11 tmnxWlanGwNumMgwHi

Table 1988: 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

Property name	Value
Default severity	minor
Source stream	main
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.

84.12 tmnxWlanGwQosRadiusGtpMismatch

Table 1989: 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
Source stream	main
Message format string	There is a mismatch between the 3GPP release *$tmnxWlanGwNotify3gppRelease$* 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 tmnxWlanGwGgsnTable 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.

84.13 tmnxWlanGwResrcProblemCause

Table 1990: 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
Source stream	main
Message format string	*$tmnxWlanGwNotifyDescription$*.
Cause	The tmnxWlanGwResrcProblemCause notification is sent to describe the cause of a WLAN Gateway resource problem.
Effect	N/A
Recovery	N/A

84.14 tmnxWlanGwResrcProblemDetected

Table 1991: 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
Source stream	main
Message format string	The status of the WLAN GW resource problem indication changed to *$tmnxWlanGwResrcProblem$*.

Property name	Value
Cause	The tmnxWlanGwResrcProblemDetected notification is sent when the value of the object tmnxWlanGwResrcProblem changes.
Effect	N/A
Recovery	N/A

84.15 tmnxWlanGwSubIfPmAddNewPlFailed

Table 1992: 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
Source stream	main
Message format string	Failed to add a new pool given by the DHCPv6 server. (service *$svc Id$*, interface *$tmnxWlanGwNotifySubIfIndex$*, address-family *$tmnx WlanGwNotifyAddrFamily$*)
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.

84.16 tmnxWlanGwSubIfPmCrIntObjFailed

Table 1993: tmnxWlanGwSubIfPmCrIntObjFailed properties

Property name	Value
Application name	WLAN_GW

Property name	Value
Event ID	2016
Event name	tmnxWlanGwSubIfPmCrIntObjFailed
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.20
Default severity	minor
Source stream	main
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.

84.17 tmnxWlanGwSubIfPmLsQryRtryFailed

Table 1994: tmnxWlanGwSubIfPmLsQryRtryFailed properties

Property name	Value
Application name	WLAN_GW
Event ID	2019
Event name	tmnxWlanGwSubIfPmLsQryRtryFailed
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.23
Default severity	minor
Source stream	main
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.

84.18 tmnxWlanGwSubIfPmNewPlReqFailed

Table 1995: 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
Source stream	main
Message format string	Failed to send a request for a new pool. (service *$svcId$*, interface *$tmnxWlanGwNotifySubIfIndex$*, address-family *$tmnxWlanGwNotifyAddrFamily$*)
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.

84.19 tmnxWlanGwSubIfPmPoolPartialUse

Table 1996: tmnxWlanGwSubIfPmPoolPartialUse properties

Property name	Value
Application name	WLAN_GW
Event ID	2021
Event name	tmnxWlanGwSubIfPmPoolPartialUse
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.25
Default severity	minor
Source stream	main

Property name	Value
Message format string	Partial usage of the server delegated prefix. (svcId *$svcId$*, subIfIndex *$tmnxWlanGwNotifySubIfIndex$*, addrFamily *$tmnxWlanGwNotifyAddrFamily$*, isaGrpId *$tmnxWlanGwNotifyIsaGrpId$*, IsaMemberId *$tmnxWlanGwNotifyIsaMemberId$*, description '*$tmnxWlanGwNotifyDescription$*')
Cause	The server delegated prefix length does not match the ISA subnet length.
Effect	An incomplete usage of the delegated prefix results in a loss of applicable IP addresses.
Recovery	Configure the delegated prefix length maximum to match the ISA subnet length.

84.20 tmnxWlanGwSubIfPmPoolTimeout

Table 1997: tmnxWlanGwSubIfPmPoolTimeout properties

Property name	Value
Application name	WLAN_GW
Event ID	2017
Event name	tmnxWlanGwSubIfPmPoolTimeout
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.21
Default severity	minor
Source stream	main
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.

84.21 tmnxWlanGwSubIfPmPoolUsageLow

Table 1998: 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
Source stream	main
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.

84.22 tmnxWlanGwSubIfPmStartD6cFailed

Table 1999: 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
Source stream	main
Message format string	The DHCPv6 client of the Pool Manager failed to start. (service *$svc Id$*, interface *$tmnxWlanGwNotifySubIfIndex$*, address-family *$tmnxWlanGwNotifyAddrFamily$*)
Cause	Failed to start a DHCPv6 client.
Effect	No pools can be requested for this ISA-BB.

Property name	Value
Recovery	Perform a shutdown/no shutdown of the DHCPv6 client.

84.23 tmnxWlanGwSubIfRedActiveChanged

Table 2000: 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
Source stream	main
Message format string	The WLAN Gateway function on interface $$ is now *$tmnxWlanGwSubIfRedActive$ - $tmnxWlanGwNotifyDescription$*
Cause	To be documented
Effect	To be documented
Recovery	No recovery is required on this system.

84.24 tmnxWlanGwTuQosProblem

Table 2001: 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

Property name	Value
Default severity	minor
Source stream	main
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.

84.25 tmnxWlanGwUeCreationFail

Table 2002: tmnxWlanGwUeCreationFail properties

Property name	Value
Application name	WLAN_GW
Event ID	2024
Event name	tmnxWlanGwUeCreationFail
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.28
Default severity	minor
Source stream	main
Message format string	Failed to create the WLAN Gateway UE with MacAddress *$tmnxWlanGwNotifyUeMacAddress$*.
Cause	The system issues the tmnxWlanGwUeCreationFail notification when the creation of a WLAN Gateway UE in tmnxWlanGwUeTable fails.
Effect	The WLAN Gateway UE was not created.
Recovery	Recovery may or may not be required, depending of the cause.

84.26 tmnxWlanGwUeReplacement

Table 2003: tmnxWlanGwUeReplacement properties

Property name	Value
Application name	WLAN_GW
Event ID	2025
Event name	tmnxWlanGwUeReplacement
SNMP notification prefix and OID	TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.29
Default severity	minor
Source stream	main
Message format string	Replaced the WLAN Gateway UE with MacAddress *$tmnxWlanGwNotifyUeMacAddress$*.
Cause	The system issues the tmnxWlanGwUeReplacement notification when a UE has been removed in favor of another UE.
Effect	The WLAN Gateway UE was replaced.
Recovery	Recovery may or may not be required, depending of the cause.

85 WPP

85.1 tmnxWppHostAuthenticationFailed

Table 2004: 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
Source stream	main
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. More 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.

85.2 tmnxWppPGHostAuthFailed

Table 2005: tmnxWppPGHostAuthFailed properties

Property name	Value
Application name	WPP
Event ID	2005
Event name	tmnxWppPGHostAuthFailed
SNMP notification prefix and OID	TIMETRA-WEB-PORTAL-PROTOCOL-MIB.tmnxWppNotifications.5
Default severity	warning
Source stream	main
Message format string	WPP host (portal-group *$tmnxWppPortalGroupName$*, address *$tmnxWppPGHostAddr$*) could not be authenticated - *$tmnxWppNotifyDescription$*.
Cause	The tmnxWppPGHostAuthFailed notification is sent when a WPP host could not be authenticated. More detailed information is supplied in the object tmnxWppNotifyDescription.
Effect	The corresponding row in the tmnxWppPGHostTable disappears if the value of the object tmnxWppIfRestoreDisconnected is equal to 'false'; otherwise, the value of the object tmnxWppPGHostStatus is set to 'idle'.
Recovery	The recovery action will depend on the exact failure cause, as given by the value of tmnxWppNotifyDescription.

85.3 tmnxWppPortalGroupStatChanged

Table 2006: tmnxWppPortalGroupStatChanged properties

Property name	Value
Application name	WPP
Event ID	2004
Event name	tmnxWppPortalGroupStatChanged
SNMP notification prefix and OID	TIMETRA-WEB-PORTAL-PROTOCOL-MIB.tmnxWppNotifications.4
Default severity	warning
Source stream	main

Property name	Value
Message format string	The state of portal group *$tmnxWppPortalGroupName$* has changed to (controlled router = *$tmnxWppPortalGroupStateContrRtr$*, number of interfaces = *$tmnxWppPortalGroupStateNumItfs$*).
Cause	The tmnxWppPortalGroupStatChanged notification is sent when the value of one of the objects in the tmnxWppPortalGroupStatTable changes.
Effect	No effect on the service.
Recovery	No recovery required.

85.4 tmnxWppPortalStatChanged

Table 2007: 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
Default severity	warning
Source stream	main
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.

85.5 tmnxWppPortalUnreachable

Table 2008: 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
Source stream	main
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.

Index

G

H

I

L

M

N

O

P

Q

R

S

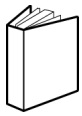
T

U

V

W

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback