



7250 Interconnect Router
7450 Ethernet Service Switch
7750 Service Router
7950 Extensible Routing System
Virtualized Service Router
Release 25.3.R1

Log Events Guide

3HE 21208 AAAA TQZZA 01
Edition: 01
March 2025

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.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2025 Nokia.

Table of contents

| | | |
|----|----------------------------|-----|
| 1 | Log events overview..... | 8 |
| 2 | ADP..... | 12 |
| 3 | ANYSEC..... | 14 |
| 4 | APPLICATION_ASSURANCE..... | 22 |
| 5 | APS..... | 66 |
| 6 | AUTO_PROV..... | 76 |
| 7 | BFD..... | 77 |
| 8 | BGP..... | 85 |
| 9 | BIER..... | 109 |
| 10 | CALLTRACE..... | 112 |
| 11 | CFLOWD..... | 115 |
| 12 | CHASSIS..... | 118 |
| 13 | DEBUG..... | 323 |
| 14 | DHCP..... | 324 |
| 15 | DHCPS..... | 341 |
| 16 | DIAMETER..... | 364 |
| 17 | DOT1X..... | 369 |
| 18 | DYNSVC..... | 370 |

| | | |
|----|----------------------------|-----|
| 19 | EFM_OAM | 371 |
| 20 | ELMI | 377 |
| 21 | ERING | 379 |
| 22 | ETH_CFM | 381 |
| 23 | ETH_TUNNEL | 390 |
| 24 | FILTER | 395 |
| 25 | GSMP | 405 |
| 26 | IGMP | 411 |
| 27 | IGMP_SNOOPING | 427 |
| 28 | IP | 434 |
| 29 | IPSEC | 441 |
| 30 | ISIS | 452 |
| 31 | L2TP | 484 |
| 32 | LAG | 490 |
| 33 | LDAP | 496 |
| 34 | LDP | 498 |
| 35 | LI | 508 |
| 36 | LLDP | 561 |
| 37 | LOGGER | 565 |

| | | |
|----|--------------------|-----|
| 38 | MACSEC..... | 581 |
| 39 | MC_REDUNDANCY..... | 593 |
| 40 | MCPATH..... | 624 |
| 41 | MGMT_CORE..... | 627 |
| 42 | MIRROR..... | 632 |
| 43 | MLD..... | 642 |
| 44 | MLD_SNOOPING..... | 657 |
| 45 | MPLS..... | 659 |
| 46 | MPLS_TP..... | 684 |
| 47 | MSDP..... | 688 |
| 48 | NAT..... | 693 |
| 49 | NTP..... | 723 |
| 50 | OAM..... | 727 |
| 51 | OPEN_FLOW..... | 746 |
| 52 | OSPF..... | 747 |
| 53 | PCAP..... | 781 |
| 54 | PCEP..... | 784 |
| 55 | PFCP..... | 785 |
| 56 | PIM..... | 788 |

| | | |
|----|-------------------|------|
| 57 | PIM_SNOOPING..... | 802 |
| 58 | PORT..... | 806 |
| 59 | PPPOE..... | 867 |
| 60 | PPPOE_CLNT..... | 873 |
| 61 | PTP..... | 875 |
| 62 | PYTHON..... | 887 |
| 63 | RADIUS..... | 888 |
| 64 | RIP..... | 891 |
| 65 | RIP_NG..... | 897 |
| 66 | ROUTE_POLICY..... | 904 |
| 67 | RPKI..... | 905 |
| 68 | RSVP..... | 907 |
| 69 | SATELLITE..... | 911 |
| 70 | SECURITY..... | 920 |
| 71 | SFLOW..... | 1036 |
| 72 | SNMP..... | 1038 |
| 73 | SR_MPLS..... | 1044 |
| 74 | SRV6..... | 1046 |
| 75 | STP..... | 1048 |

| | | |
|----|-----------------------|------|
| 76 | SVCMGR | 1068 |
| 77 | SYSTEM | 1210 |
| 78 | TLS | 1264 |
| 79 | TREE_SID | 1267 |
| 80 | USER | 1274 |
| 81 | VIDEO | 1287 |
| 82 | VRRP | 1313 |
| 83 | VRTR | 1327 |
| 84 | WLAN_GW | 1373 |
| 85 | WPP | 1390 |
| | Index | 1394 |

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: <ul style="list-style-type: none"> 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 <p> 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.</p> |
| <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 |
|-------|---|
| | <p>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.</p> <p>For further information about variables found in the <message> strings, please see the associated SNMP Notification definition in the SR OS MIBs.</p> |

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. <ul style="list-style-type: none"> critical major minor warning cleared |
| Source stream | The event source. <ul style="list-style-type: none"> 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 <i>\$tmnxAnySecMkaStatsOperStateNotif\$</i> - Encryption Group: <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> , Remote Peer: <i>\$tmnxAnySecPeerAddrNotif\$</i> , CAK Name: <i>\$tmnxAnySecCakNameNotif\$</i> |
| 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: <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> , Remote Peer: <i>\$tmnxAnySecPeerAddrNotif\$</i> , CAK Name: <i>\$tmnxAnySecNewCakNameNotif\$</i> , Key Entry Number: <i>\$tmnxAnySecKeyEntryNumberNotif\$</i> |
| 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 <i>\$tmnxAnySecPeerAddr\$</i> in encryption group <i>\$tmnxAnySecEncryptGrpName\$</i> with MI:SCI <i>\$tmnxAnySecMkaStatsMemberId\$</i> : <i>\$tmnxAnySecMkaStatsOutboundSci\$</i> CA <i>\$tmnxAnySecEncryptGrpCName\$</i> peer MI <i>\$tmnxAnySecPeerMemberIdNotif\$</i> |

| 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 <i>\$tmnxAnySecPeerAddr\$</i> in encryption group <i>\$tmnxAnySecEncryptGrpName\$</i> with MI:SCI <i>\$tmnxAnySecMkaStatsMemberId\$:\$tmnxAnySecMkaStatsOutboundSci\$ CA \$tmnxAnySecEncryptGrpCAName\$</i> local key-server priority <i>\$tmnxAnySecMkaLocalKSPrioNotif\$</i> peer key-server priority <i>\$tmnxAnySecMkaPeerKSPrioNotif\$</i> cipher-suite <i>\$tmnxAnySecMkaStatsOperCipher\$</i> peer MI <i>\$tmnxAnySecPeerMemberIdNotif\$</i> |
| 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 <i>\$tmnxAnySecPeerAddrNotif\$</i> in encryption group <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> |
| Cause | The <i>tmnxAnySecMkaSessionInitiation</i> 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 <i>tmnxAnySecMkaOperState Changed</i> 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 <i>\$tmnxAnySecPeerAddrNotif\$</i> in encryption group <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> - <i>\$tmnxAnySecMkaSessTermReasonNotif\$</i> is administratively disabled - traffic is being dropped |
| Cause | The <i>tmnxAnySecMkaSessionTermination</i> 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 <i>tmnxAnySecSessionDisabled</i> 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 | <i>tmnxAnySecPeerInconsisRxSciClrd</i> |
| SNMP notification prefix and OID | TIMETRA-ANYSEC-MIB. <i>tmnxAnySecNotifications.8</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | ANYsec inconsistent Rx SCI cleared - transmission to peer <i>\$tmnxAnySecPeerAddrNotif\$</i> in encryption group <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> resumed |
| Cause | The <i>tmnxAnySecPeerInconsisRxSciClrd</i> notification is sent when the condition that caused the previous <i>tmnxAnySecPeerInconsisRxSciDtctd</i> 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 <i>\$tmnxAnySecPeerAddrNotif\$</i> in encryption group <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> stopped - Rx SCI: <i>\$tmnxAnySecPeerIncsRxSciNotif\$</i> - reason: <i>\$tmnxAnySecPeerIncsRxSciResnNotif\$</i> |
| 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 <i>\$tmnxAnySecPeerAddrNotif\$</i> (peer admin state: <i>\$tmnxAnySecPeerAdminState\$</i>) in encryption group <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> (group admin state: <i>\$tmnxAnySecEncryptGrpAdminState\$</i>) - 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 <i>\$tmnxAnySecPeerAddrNotif\$</i> in encryption group <i>\$tmnxAnySecEncryptGroupNameNotif\$</i> |
| 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 <i>\$tmnxBsxAarpInstId\$</i> changed operational state: <i>\$tmnxBsxAarpInstOperState\$</i> , flags = <i>\$tmnxBsxAarpInstOperFlags\$</i> |
| 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 <i>\$tmnxBsxAarpInstId\$</i> changed state: <i>\$tmnxBsxAarpInstState\$</i> , flags = <i>\$tmnxBsxAarpInstOperFlags\$</i> |
| 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> . |
| 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 <i>\$tmnxBsxNotifyAaSubscriberName\$</i> . |
| Cause | A <i>tmnxBsxAaSubscriberAcctDataLoss</i> 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 | <i>tmnxBsxAaSubscribersUnassigned</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.11</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | ISA-AA group <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> has unassigned subscribers |
| Cause | A <i>tmnxBsxAaSubscribersUnassigned</i> 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 <i>\$tmnxBsxNotifyCertProfileName\$</i> in ISA-AA Group <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> is <i>\$tmnxBsxNotifyCertProfOperState\$</i> . Reason: <i>\$tmnxBsxNotifyReason\$</i> |
| Cause | A tmnxBsxCertProfileOperStateChngd notification is generated when the operational state of the certificate-profile is changed. The tmnxBsxNotifyReason 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 <i>\$tmnxBsxDatapathCpuHighWatermark\$%</i> on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> in group <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> . |
| Cause | A <i>tmnxBsxDatapathCpuUsage</i> notification is generated when the current datapath CPU usage on the MDA in the ISA-AA group is greater than or equal to the <i>tmnxBsxDatapathCpuHighWatermark</i> 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 <i>tmnxBsxIsaAaGrpOverloadCutThru</i> 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 | <i>tmnxBsxDatapathCpuUsageClear</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.59</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Datapath CPU usage is less than or equal to <i>\$tmnxBsxDatapathCpuLowWatermark\$%</i> on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> in group <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> . |
| Cause | A <i>tmnxBsxDatapathCpuUsageClear</i> notification is generated to indicate a prior <i>tmnxBsxDatapathCpuUsage</i> 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 <i>tmnxBsxDatapathCpuLowWatermark</i> . |
| Effect | The <i>tmnxBsxDatapathCpuUsage</i> 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> DNS IP Cache " <i>\$tmnxBsxDnsIpCacheName\$</i> " for ISA-MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> is greater than or equal to the <i>\$tmnxBsxDnsIpCacheHighWatermark\$</i> % high watermark. The cache size is <i>\$tmnxBsxDnsIpCacheSize\$</i> . |
| 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> DNS IP Cache " <i>\$tmnxBsxDnsIpCacheName\$</i> " for ISA-MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> is less than or equal to the <i>\$tmnxBsxDnsIpCacheLowWatermark\$</i> % low watermark. The cache size is <i>\$tmnxBsxDnsIpCacheSize\$</i> . |
| Cause | A tmnxBsxDnsIpCacheFullClear notification is generated when the number of entries in a DNS IP Cache is less than or equal to the percentage value tmnxBsxDnsIpCacheLowWatermark of its tmnxBsxDnsIpCacheSize and the previous percentage value was greater than this threshold. |
| Effect | The DNS IP Cache is no longer relatively close to being full. |
| Recovery | No recovery is required. |

4.12 tmnxBsxHttpUriParamLimitExceeded

Table 27: *tmnxBsxHttpUriParamLimitExceeded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | APPLICATION_ASSURANCE |
| Event ID | 4441 |
| Event name | tmnxBsxHttpUriParamLimitExceeded |
| 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> , reason: <i>\$tmnxBsxNotifyReason\$</i> |
| Cause | A <i>tmnxBsxHttpUrlParamLimitExceeded</i> notification is generated when the group limit of unique <i>tmnxBsxAaSubHttpUrlParam</i> values has been exceeded. The <i>tmnxBsxNotifyReason</i> 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 | <i>tmnxBsxIsaAaGrpBitRate</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.19</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Bit rate is greater than or equal to <i>\$tmnxBsxBitRateHighWatermark\$</i> megabits/s on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> . |
| Cause | A <i>tmnxBsxIsaAaGrpBitRate</i> notification is generated when the current bit rate on the MDA in the ISA-AA group is greater than or equal to the <i>tmnxBsxBitRateHighWatermark</i> 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 <i>\$tmnxBsxBitRateLowWatermark</i> \$ megabits/s on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> 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 $tmnxBsxIsaAaGrpCapCostHighThres$ 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-sub, 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> 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::tmnxBsxIsaAaGrpFailToMode 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> flow record usage is greater than or equal to high watermark. The Active ISA-AA MDA is <i>\$tmnxBsxNotifyIsaMdaNum\$</i> |
| 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> flow record usage is less than or equal to low watermark. The Active ISA-AA MDA is <i>\$tmnxBsxNotifyIsaMdaNum\$</i> |
| Cause | The conditions that caused tmnxBsxIsaAaGrpFlowFull or tmnxBsxIsaAaGrpFlowFull 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 <i>\$tmnxBsxFlowSetupHighWatermark\$</i> flows/s on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> . |
| Cause | A <i>tmnxBsxIsaAaGrpFlowSetup</i> notification is generated when the current flow setup rate on the MDA in the ISA-AA group is greater than or equal to <i>tmnxBsxFlowSetupHighWatermark</i> 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 | <i>tmnxBsxIsaAaGrpFlowSetupClear</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.16</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Flow setup rate is less than or equal to <i>\$tmnxBsxFlowSetupLowWatermark\$</i> flows/s on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> or corresponding <i>tmnxBsxIsaAaGrpFlowSetup</i> notification has been disabled. |
| Cause | A <i>tmnxBsxIsaAaGrpFlowSetupClear</i> notification is generated to indicate a prior <i>tmnxBsxIsaAaGrpFlowSetup</i> 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 <i>tmnxBsxFlowSetupLowWatermark</i> . 2. The corresponding <i>tmnxBsxIsaAaGrpFlowSetup</i> notification has been disabled by raising the <i>tmnxBsxFlowSetupHighWatermark</i> 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> MDA <i>\$tmnxBsxNotifyActiveMda\$</i> wa-shared buffer use is greater than or equal to <i>\$tmnxBsxIsaAaGrpFromSubWaSBfHiWmk\$</i> 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> MDA <i>\$tmnxBsxNotifyActiveMda\$</i> wa-shared buffer use is less than or equal to <i>\$tmnxBsxIsaAaGrpFromSubWaSBfLoWmk\$</i> in the from-subscriber direction or corresponding <i>tmnxBsxIsaAaGrpFmSbWaSBufOvld</i> notification has been disabled. |
| Cause | A <i>tmnxBsxIsaAaGrpFmSbWaSBufOvldClr</i> is generated to indicate a prior <i>tmnxBsxIsaAaGrpFmSbWaSBufOvld</i> 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 <i>tmnxBsxIsaAaGrpFmSbWaSBufOvld</i> notification has been disabled by raising the <i>tmnxBsxIsaAaGrpFromSubWaSBfHiWmk</i> 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> 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 <i>\$tmnxBsxPacketRateHighWatermark\$</i> packets/s on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> . |
| 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 <i>\$tmnxBsxPacketRateLow Watermark\$</i> packets/s on ISA-AA MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> 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 tmnxBsxPacketRateLowWatermark. 2. The corresponding tmnxBsxIsaAaGrpPacketRate notification has been disabled by raising the tmnxBsxPacketRateHighWatermark 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> has switched activity. The Active ISA-AA MDA is now <i>\$tmnxBsxNotifyIsaMdaNum\$</i> |
| 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> MDA <i>\$tmnxBsxNotifyActiveMda\$</i> wa-shared buffer use is greater than or equal to <i>\$tmnxBsxIsaAaGrpToSubWaSBfHiWmk\$</i> 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 \$tmnxBsxNotifyActive Mda\$ wa-shared buffer use is less than or equal to \$tmnxBsxIsaAaGrp ToSubWaSBfLoWmk\$ 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 tmnxBsxIsaAaGrp ToSubWaSBfHiWmk 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 <i>\$tmnxBsxNotifyIsaAaGroupIndex\$</i> , <i>\$tmnxBsxNotifyActionStatus\$</i> |
| 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: <i>\$tmnxBsxNotifyReason\$</i> . |
| 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> with reason: <i>\$tmnxBsxNotifyReason\$</i> . |
| 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 tmnxBsxNotifyReason 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 <i>\$tmnxBsxRadApName\$</i> with reason: <i>\$tmnxBsxNotifyReason\$</i> . |
| 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 <i>\$tmnxBsxRadApIntrmUpdateInterval\$</i> 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 \$tmnxBsxRadApServIndex\$ 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 'outOfService' 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$ \$tmnxBsxNotifyTcaCfgFilterType\$ "\$tmnxBsxNotifyTcaCfgFilterName\$" entry \$tmnxBsxNotifyTcaFtrEnCfgEntryId\$ in the \$tmnxBsxNotifyTcaCfgDirection\$ direction (\$tmnxBsxNotifyReason\$).</i> |
| 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 tmnxBsxStatTcaFtrEnCfgLoWmark 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$ \$tmnxBsxNotifyTcaCfgFilterType\$ "\$tmnxBsxNotifyTcaCfgFilterName\$" entry \$tmnxBsxNotifyTcaFtrEnCfgEntryId\$ in the \$tmnxBsxNotifyTcaCfgDirection\$ direction (\$tmnxBsxNotifyReason\$).</i> |

| 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 tmnxBsxStatTcaFtrEnCfgHiWmark 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> <i>\$tmnxBsxNotifyTcaCfgFilterType\$</i> " <i>\$tmnxBsxNotifyTcaCfgFilterName\$</i> " <i>\$tmnxBsxNotifyTcaCfgFltrWmarkType\$</i> in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| 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 tmnxBsxNotifyReason 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> <i>\$tmnxBsxNotifyTcaCfgFilterType\$</i> " <i>\$tmnxBsxNotifyTcaCfgFilterName\$</i> " <i>\$tmnxBsxNotifyTcaCfgFltrWmarkType\$</i> in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| 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 tmnxBsxNotifyReason 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> policer " <i>\$tmnxBsxNotifyTcaPolicerName\$</i> " in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| Cause | A <i>tmnxBsxStatPolcrTcaThreshCrClear</i> notification is generated when the utilization matching a <i>tmnxBsxStatTcaPolcrCfgEntry</i> in the past minute is less than or equal to the value of <i>tmnxBsxStatTcaPolcrCfgLoWmark</i> and <i>tmnxBsxStatPolcrTcaThreshCrossed</i> is currently raised. The <i>tmnxBsxNotifyReason</i> will identify the utilization. |
| Effect | The <i>tmnxBsxStatPolcrTcaThreshCrossed</i> 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 | <i>tmnxBsxStatPolcrTcaThreshCrossed</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.51</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Threshold Crossing Alert raised for ISA-AA Group <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> policer " <i>\$tmnxBsxNotifyTcaPolicerName\$</i> " in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| Cause | A <i>tmnxBsxStatPolcrTcaThreshCrossed</i> notification is generated when the utilization matching a <i>tmnxBsxStatTcaPolcrCfgEntry</i> in the past minute is greater than or equal to the value of <i>tmnxBsxStatTcaPolcrCfgHiWmark</i> and the notification is not currently raised for the same entry. The <i>tmnxBsxNotifyReason</i> 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> <i>\$tmnxBsxNotifyTcaCfgType\$</i> in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$ \$tmnxBsxNotifyTcaCfgType\$</i> in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| 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 <i>\$tmnxBsxNotifySubFailedAction\$</i> a subscriber in group <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> on ISA-MDA <i>\$tmnxBsxNotifyIsaMdaNum\$</i> with reason: <i>\$tmnxBsxNotifyReason\$</i> . |
| 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 | <i>\$tmnxBsxAaSubscriberType\$</i> subscriber <i>\$tmnxBsxAaSubscriber\$</i> 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 | <i>\$tmnxBsxAaSubscriberType\$</i> subscriber <i>\$tmnxBsxAaSubscriber\$</i> removed from quarantine |
| Cause | A <i>tmnxBsxSubQuarantined</i> notification is generated when a subscriber exits quarantined state. |
| Effect | The <i>tmnxBsxTcpValTcaCrossed</i> 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> TCP validate " <i>\$tmnxBsxNotifyTcpValTcaName\$</i> " in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |

| 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 tmnxBsxNotifyReason 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> TCP validate " <i>\$tmnxBsxNotifyTcpValTcaName\$</i> " in the <i>\$tmnxBsxNotifyTcaCfgDirection\$</i> direction (<i>\$tmnxBsxNotifyReason\$</i>). |
| Cause | A tmnxBsxTcpValTcaCrossedClear notification is generated when the utilization matching a tmnxBsxTcpValTcaEntry in the past minute is less than or equal to the value of tmnxBsxTcpValTcaLowWatermark and tmnxBsxTcpValTcaCrossed is currently raised. The tmnxBsxNotifyReason will identify the utilization. |
| Effect | The tmnxBsxTcpValTcaCrossed notification is cleared. |
| Recovery | There is no recovery for this notification. |

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 <i>\$tmnxBsxNotifyAaSubscriberName\$</i> has been created in group-partition <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> . |
| 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 <i>\$tmnxBsxNotifyAaSubscriberName\$</i> has been deleted from group-partition <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> <i>\$tmnxBsxNotifyReason\$</i> . |
| Cause | A <i>tmnxBsxTransIpPolAaSubDeleted</i> 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 | <i>tmnxBsxTransIpPolDhcpAddWarning</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.26</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Problem encountered while attempting to add a transit subscriber to group-partition <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> : <i>\$tmnxBsxNotifyReason\$</i> . |
| Cause | A <i>tmnxBsxTransIpPolDhcpAddWarning</i> 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 <i>tmnxBsxNotifyReason</i> 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> : <i>\$tmnxBsxNotifyReason\$</i> . |
| 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> : <i>\$tmnxBsxNotifyReason\$</i> . |
| Cause | A <i>tmnxBsxTransIpPolDiamGxError</i> 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 <i>tmnxBsxNotifyReason</i> 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 | <i>tmnxBsxTransIpPolRadCoAAudit</i> |
| SNMP notification prefix and OID | TIMETRA-BSX-NG-MIB. <i>tmnxBsxNotifications.23</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | CoA audit for group-partition <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> is in state <i>\$tmnxBsxNotifyRadiusCoAAuditState\$</i> . |
| Cause | A <i>tmnxBsxTransIpPolRadCoAAudit</i> 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> : <i>\$tmnxBsxNotifyReason\$</i> . |
| 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> : <i>\$tmnxBsxNotifyReason\$</i> . |
| Cause | A <i>tmnxBsxTransitIpPolRadDiscError</i> notification is generated when an error occurs while processing a Disconnect request from a RADIUS server. The <i>tmnxBsxNotifyReason</i> 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 <i>\$tmnxBsxNotifyAaGrpPartIndex\$</i> transit IP policy <i>\$tmnxBsxNotifyTransitIpPolicyId\$</i> : <i>\$tmnxBsxNotifyReason\$</i> . |
| Cause | A <i>tmnxBsxTransitIpPersistenceWarn</i> notification is generated when a problem occurs while attempting to register a dynamic transit subscriber address with the persistence infrastructure. The <i>tmnxBsxNotifyReason</i> 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> URL Filter <i>\$tmnxBsxUrlFilterName\$</i> state changed to <i>\$tmnxBsxUrlFltrOperState\$</i> , flags = <i>\$tmnxBsxUrlFltrOperFlags\$</i> . |
| 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 <i>\$tmnxBsxIsaAaGroupIndex\$</i> URL Filter <i>\$tmnxBsxUrlFilterName\$</i> DNS server state changed to <i>\$tmnxBsxUrlFtrWebSvDnsOperState\$</i> , flags = <i>\$tmnxBsxUrlFtrWebSvDnsOperFlags\$</i> . |
| Cause | The <i>tmnxBsxUrlFtrWebServOprStateChg</i> notification is generated when the operational status of a URL Filter Web Service DNS Server has transitioned either from 'inService' to 'outOfService' or from 'outOfService' 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 " <i>\$tmnxBsxUrlListName\$</i> " in ISA-AA group <i>\$tmnxBsxIsaAaGroupIndex\$</i> has failed. The current operational state is: <i>\$tmnxBsxUrlListStatusOperState\$</i> , flags = <i>\$tmnxBsxUrlListStatusOperFlags\$</i> . |
| Cause | A <i>tmnxBsxUrlListFailure</i> 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 'outOfService (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 tmnxBsxUrlListFileUrl, and use tmnxBsxUrlListAdminState or tmnxBsxUrlListUpgrade 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 \$tmnxBsxIsaAaGroupIndex\$ has been updated. There are \$tmnxBsxUrlListStatusNumEntries\$ 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 <i>\$subject\$</i> . |

| 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 - <i>\$apsCommandSwitch\$</i> 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, forcedSwitchWorkToProtect, forcedSwitchProtectToWork, manualSwitchWorkToProtect, 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 <i>\$tApsMcApsCtlLinkState\$</i> |
| 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 <i>\$apsStatusK1K2Trans\$</i> . |
| 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 - <i>\$apsCommandSwitch\$</i> 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 - <i>\$apsCommandSwitch\$</i> 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 | <i>\$subject\$: \$title\$</i> <i>\$message\$</i> |
| 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 <i>\$tmnxBfdOnLspExtSessLinkType\$</i> BFD Session with Local Discriminator <i>\$tmnxBfdOnLspExtSessLclDisc\$</i> on <i>\$subject\$</i> 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 <i>\$tmnxBfdOnLspExtSessLinkType\$</i> BFD session with Local Discriminator <i>\$tmnxBfdOnLspExtSessLclDisc\$</i> on <i>\$subject\$</i> is down due to <i>\$tmnxBfdOnLspExtSessOperFlags\$</i> |
| 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 <i>\$tmnxBfdOnLspExtSessLinkType\$</i> BFD session with local discriminator <i>\$tmnxBfdOnLspExtSessLclDisc\$</i> on <i>\$subject\$</i> 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::vRtrIbfBfdExtType), 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 (<i>\$tmnxBfdOnLspExtSessChngdProtocol\$</i>) using BFD session on node <i>\$subject\$</i> has been <i>\$tmnxBfdOnLspExtSessProtoChngdSta\$</i> |
| Cause | The tmnxBfdOnLspExtSessProtChange notification is generated when there is a change in the list of protocols specified by tmnxBfdOnLspExtSessProtocols 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 <i>\$tmnxBfdOnLspExtSessLinkType\$</i> BFD session with Local Discriminator <i>\$tmnxBfdOnLspExtSessLclDisc\$</i> on <i>\$subject\$</i> 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 <i>\$tmnxBfdOnLspSessLinkType\$</i> BFD Session with Local Discriminator <i>\$tmnxBfdOnLspSessLclDisc\$</i> on <i>\$subject\$</i> 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 <i>\$tmnxBfdOnLspSessLinkType\$</i> BFD session with Local Discriminator <i>\$tmnxBfdOnLspSessLclDisc\$</i> on <i>\$subject\$</i> is down due to <i>\$tmnxBfdOnLspSessOperFlags\$</i> |
| 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 <i>\$tmnxBfdOnLspSessLinkType\$</i> BFD session with local discriminator <i>\$tmnxBfdOnLspSessLcIDisc\$</i> on <i>\$subject\$</i> 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 <code>tmnxBfdOnLspSessNoTailResources</code> 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 <code>TIMETRA-VRTR-MIB::vRtrLspBfdSession</code> is 'enabled(1)', the system limit on the number of session tail ends is <code>TIMETRA-VRTR-MIB::vRtrLspBfdMaxSessions</code> . If <code>TIMETRA-VRTR-MIB::vRtrLspBfdSession</code> 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, <code>tmnxBfdOnLspSessNoTailResources</code> is raised, and a ten minute timer is started. When the timer expires, 1. <code>tmnxBfdOnLspSessNoTailResources</code> 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 <code>TIMETRA-VRTR-MIB::vRtrLspBfdSession</code> and/or <code>TIMETRA-VRTR-MIB::vRtrLspBfdMaxSessions</code> restarts the process at the initial state. |
| Effect | One or more BFD on LSP sessions could not be established. |
| Recovery | Change <code>TIMETRA-VRTR-MIB::vRtrLspBfdSession</code> to 'enabled(1)', or increase <code>TIMETRA-VRTR-MIB::vRtrLspBfdMaxSessions</code> , 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 | <code>tmnxBfdOnLspSessProtChange</code> |
| SNMP notification prefix and OID | <code>TIMETRA-BFD-MIB.tmnxBfdNotifications.4</code> |
| Default severity | minor |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | The protocol (<i>\$tmnxBfdOnLspSessChangedProtocol\$</i>) using BFD session on node <i>\$subject\$</i> has been <i>\$tmnxBfdOnLspSessProtoChngdState\$</i> |
| Cause | The <i>tmnxBfdOnLspSessProtChange</i> notification is generated when there is a change in the list of protocols specified by <i>tmnxBfdOnLspSessProtocols</i> 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 | <i>tmnxBfdOnLspSessUp</i> |
| SNMP notification prefix and OID | TIMETRA-BFD-MIB. <i>tmnxBfdNotifications.2</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | The <i>\$tmnxBfdOnLspSessLinkType\$</i> BFD session with Local Discriminator <i>\$tmnxBfdOnLspSessLclDisc\$</i> on <i>\$subject\$</i> is up |
| Cause | The <i>tmnxBfdOnLspSessUp</i> 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 | <i>\$subject\$</i> : BGP - <i>\$field\$</i> configuration ignored - <i>\$reason\$</i> |
| 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 | <i>\$subject\$</i> : BGP connection manager for address family <i>\$addr_family_str\$</i> 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : 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 <i>\$tBgpASN4Byte\$</i>) <i>\$subject\$</i> : Closing connection: <i>\$peer_ip_str\$</i> 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : inbound connection rejected because the BGP peer received connection attempt on <i>\$src_addr_str\$</i> but it only accepts connection on <i>\$lcl_addr_str\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : 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 | <i>\$subject\$</i> : 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 | <i>\$subject\$</i> : trying to set <i>\$varname\$</i> to <i>\$tryval\$</i> - valid range is [<i>\$minval\$</i> - <i>\$maxval\$</i>] - setting to <i>\$finalval\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : received notification: code <i>\$code_str\$</i> subcode <i>\$subcode_str\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : sending notification: code <i>\$code_str\$</i> subcode <i>\$subcode_str\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$vRtrID\$</i> : Discarded path attribute received from BGP Peer <i>\$tBgpPeerNgAddr\$</i> with attribute type [<i>\$tBgp4PathAttrType\$</i>] and length [<i>\$tBgp4PathAttrLength\$</i>]. Hex dump: <i>\$tBgp4PathAttribute\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$vRtrID\$</i> : BGP Peer <i>\$tBgpPeerNgAddr\$</i> : Invalid path attribute received with attribute type [<i>\$tBgp4PathAttrType\$</i>] and length [<i>\$tBgp4PathAttrLength\$</i>]. Hex dump: <i>\$tBgp4PathAttribute\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$vRtrID\$</i> : BGP Peer: <i>\$tBgpPeerNgAddr\$</i> . Hex dump: <i>\$tBgp4UpdateMessage\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$vRtrID\$</i> : BGP Peer: <i>\$tBgpPeerNgAddr\$</i> , Route: <i>\$tBgp4WithdrawnRoutePrefix\$</i> 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 | <i>\$bgp_peer_name\$</i> : 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : Flowspec NLRI - unsupported community action : [<i>\$tBgpFlowspecExtCommunityAction\$</i>], action value : [<i>\$tBgpFlowspecExtCommActionValue\$</i>] 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 | <i>\$subject\$</i> : <i>\$title\$</i> <i>\$message\$</i> |
| 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 | <i>\$bgp_peer_name\$</i> : Closing connection: reached dynamic peer limit (<i>\$tBgpInstanceDynamicPeerLimit\$</i>) for BGP instance <i>\$tBgpInstanceIndex\$</i> |
| 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 <i>\$tBgpConvergenceFamily\$</i> transitioned from <i>\$tBgpOldConvergenceState\$</i> to <i>\$tBgpConvergenceState\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : number of routes learned has exceeded configured maximum (<i>\$tBgpPeerNgPfxLmtMaxPrefix\$</i>) for <i>\$tBgpPeerNgPfxLmtFamily\$</i> 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 (tBgpPeerNgPfxLmtMaxPrefix). 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 \$tBgpPeerNgPfxLmtFamily\$ family |
| Cause | A tBgpMaxNgPfxLmtThresholdReached notification is generated when the number of routes learned from the peer has exceeded tBgpPeerNgPfxLmtThreshold percent of the configured maximum (tBgpPeerNgPfxLmtMaxPrefix). |
| Effect | No direct effect but if the peer continues to advertise more routes then the number of routes may exceed the configured maximum (tBgpPeerNgPfxLmtMaxPrefix). 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : moved from higher state <i>\$old_state_str\$</i> to lower state <i>\$new_state_str\$</i> due to event <i>\$event_str\$</i> |
| 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 <i>\$tBgpASN4Byte\$</i>) <i>\$bgp_peer_name\$</i> : 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 \$tBgpPeerNgMinHoldTime\$ |
| Cause | The BGP peer tried to establish a peering with a hold time less than the configured minimum hold time value. |
| Effect | The BGP peering is rejected. |
| Recovery | Establish peering with a hold time equal to or greater than the minimum hold time configured. |

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 | <i>\$bgp_peer_name\$</i> : Closing connection: reached dynamic peer limit (<i>\$tBgpPGDynamicPeerLimit\$</i>) for BGP group <i>\$tBgpPeerGroupName\$</i> |
| 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 | <i>\$bgp_peer_name\$</i> : Closing connection: reached max sessions limit (<i>\$tBgpPGDynNbrIfMaxSessions\$</i>) for interface <i>\$tBgpPGDynNbrInterfaceIndex\$</i> |
| 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 <i>\$tBgp4BadErrorMessageType\$</i> the message received is <i>\$tBgp4BadErrorMessage\$</i> . |
| 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 <i>\$tmnxBmpSessionChangeVRtrID\$</i> : Station <i>\$tmnxBmpSessionChangeStationName\$</i> moved from state <i>\$tmnxBmpSessionChangeOldState\$</i> to state <i>\$tmnxBmpSessionChangeNewState\$</i> due to reason: <i>\$tmnxBmpSessionChangeReason\$</i> |
| 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 vRtrBierBfrldCollision

Table 144: vRtrBierBfrldCollision properties

| Property name | Value |
|----------------------------------|---|
| Application name | BIER |
| Event ID | 2001 |
| Event name | vRtrBierBfrldCollision |
| SNMP notification prefix and OID | TIMETRA-BIER-MIB.vRtrBierNotifications.1 |
| Default severity | minor |
| Source stream | main |
| Message format string | Same BFR id <i>\$vRtrBierNotifyBfrld\$</i> received from <i>\$vRtrBierPrefix1Address\$</i> and <i>\$vRtrBierPrefix2Address\$</i> by the sub-domain <i>\$vRtrBierNotifySubDomainId\$</i> with BSL <i>\$vRtrBierNotifyBsl\$</i> |
| Cause | The vRtrBierBfrldCollision 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 <i>\$vRtrBierNotifyRecvMTId\$</i> received by the sub-domain <i>\$vRtrBierNotifySubDomainId\$</i> with BSL <i>\$vRtrBierNotifyBsl\$</i> and multi-topology <i>\$vRtrBierNotifyMTId\$</i> |
| 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 <i>\$vRtrBierNotifyRecvSubDomainId\$</i> received by the sub-domain <i>\$vRtrBierNotifySubDomainId\$</i> with BSL <i>\$vRtrBierNotifyBsl\$</i> |
| 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 <i>\$vRtrBierNextHopeType\$</i> is not supported for the given prefix <i>\$vRtrBierPrefix1Address\$</i> , next-hop address <i>\$vRtrBierNextHopAddress\$</i> and outgoing interface <i>\$vRtrIfIndex\$</i> |
| 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 | <i>\$subject\$: \$title\$</i> <i>\$message\$</i> |
| 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 (<i>\$tmnxCallTraceLocationSizeLimit\$</i> MB) of all call trace log files on 'cf <i>\$tmnxCallTraceLocationCFlashId\$</i> ' 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 tmnxCallTraceLocationSizeLimit) 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 <i>\$tmnxCallTraceMaxFilesNumber\$</i> 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 tmnCflowdCreateFailure

Table 151: tmnCflowdCreateFailure properties

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

11.2 tmnCflowdFlowCreateFailure

Table 152: tmnCflowdFlowCreateFailure properties

| Property name | Value |
|----------------------------------|---|
| Application name | CFLOWD |
| Event ID | 2006 |
| Event name | tmnCflowdFlowCreateFailure |
| SNMP notification prefix and OID | TIMETRA-CFLOWD-MIB.tmnCflowdNotifications.6 |

| Property name | Value |
|-----------------------|--|
| Default severity | minor |
| Source stream | main |
| Message format string | Cflowd flow creation failed - <i>\$tmnxCflowdFlowFailureReasonCode\$</i> |
| 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 <i>\$tmnxCFHostCollAddress \$:\$tmnxCFHostCollUdpPort\$ Version \$tmnxCFHostCollVersion\$ - Reason: \$tmnxCflowdFlowFailureReasonCode\$</i> |
| 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: <i>\$tmnxCflowdAdmin Status\$</i> , operational state: <i>\$tmnxCflowdOperStatus\$</i> |
| 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.tmxCpmIcPort Notifications.7 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF DDM checksums do not match |
| Cause | The tmxCpmIcPortSFFStatusFailure notification is generated when the value of tmxCpmIcPortSFFStatus 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 | CpmlcPortSFFStatusFailure |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.7 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF checksums do not match |
| Cause | The tmnxCpmlcPortSFFStatusFailure notification is generated when the value of tmnxCpmlcPortSFFStatus 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 CpmlcPortSFFStatusReadError

Table 157: CpmlcPortSFFStatusReadError properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4013 |
| Event name | CpmlcPortSFFStatusReadError |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.7 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF read failure |
| Cause | The tmnxCpmlcPortSFFStatusFailure notification is generated when the value of tmnxCpmlcPortSFFStatus 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 tmnxSfmlcPortSFFStatusFailure notification is generated when the value of tmnxSfmlcPortSFFStatus 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 SfmlcPortSFFStatusReadError

Table 161: SfmlcPortSFFStatusReadError properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4023 |
| Event name | SfmlcPortSFFStatusReadError |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.5 |
| Default severity | minor |
| Source stream | main |
| Message format string | SFM interconnect port SFF read failure |
| Cause | The tmnxSfmlcPortSFFStatusFailure notification is generated when the value of tmnxSfmlcPortSFFStatus 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : 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 | <i>\$tmnxChassisNotifyHwIndex\$</i> : 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 <i>\$tmnxEsaNotifyId\$</i> / <i>\$tmnxEsaVmNotifyId\$</i> 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 <i>\$tmnxEsaNotifyId\$/\$tmnxEsaVmNotifyId\$</i> 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 <i>\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> 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: tIPseclsaMemLowWatermark properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2150 |
| Event name | tIPseclsaMemLowWatermark |
| 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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxMDASlotNum\$</i> has dropped back to the normal level. |
| Cause | A tIPseclsaMemLowWatermark 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 tIPseclsaMemMax

Table 172: tIPseclsaMemMax properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2152 |
| Event name | tIPseclsaMemMax |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.139 |
| Default severity | minor |
| Source stream | main |
| Message format string | The memory usage for ISA <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxMDASlotNum\$</i> has reached the maximum value. |
| Cause | A tIPseclsaMemMax 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 <i>\$tmnxHwClass\$</i> : alarm input voltage failure |
| Cause | A <i>tmnxAlarmInputVoltageFailure</i> notification is sent when the internal power supply for alarm inputs fails. The value of <i>tmnxSasAlarmInputPowerStatus</i> 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 <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> got <i>\$tmnxBluetoothModuleConnected\$</i> to <i>\$tmnxBluetoothModuleConnectedMac\$</i> . |
| 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 <i>\$tmnxMacScaleCardSlotNum\$</i> 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 <i>\$tmnxMacScaleCardSlotNum\$</i> 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : system in anti-theft mode has been unlocked |
| Cause | The tmnxChassisAntiTheftUnlocked notification is generated to indicate that the system has successfully been unlocked following a reboot while Anti-Theft mode was enabled. |
| Effect | N/A |
| Recovery | N/A |

12.25 tmnxChassisGoldenStatusEvent

Table 179: *tmnxChassisGoldenStatusEvent* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 6018 |
| Event name | tmnxChassisGoldenStatusEvent |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotifications.315 |
| Default severity | critical |
| Source stream | main |
| Message format string | CPM <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> active to backup BIOS copy failed. Not retrying. |
| Cause | The tmnxChassisGoldenStatusEvent is sent when the backup BIOS update was unsuccessful. BIOS fails to program BACKUP or ACTIVE BIOS SPI FLASH. |
| Effect | There is no redundancy if the active BIOS fails. |
| Recovery | Contact Nokia customer support. |

12.26 tmnxChassisHiBwMcastAlarm

Table 180: *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 |

| Property name | Value |
|-----------------------|--|
| Message format string | Class <i>\$tmnxHwClass\$</i> : Plane shared by multiple multicast high bandwidth taps |
| Cause | The <i>tmnxChassisHiBwMcastAlarm</i> notification is generated when a plane is shared by more than one high bandwidth multicast tap. |
| Effect | N/A |
| Recovery | N/A |

12.27 tmnxChassisNotificationClear

Table 181: *tmnxChassisNotificationClear* properties

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

12.28 tmnxChassisUpgradeComplete

Table 182: *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 <i>\$tmnxHwClass\$</i> : 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 |

12.29 tmnxChassisUpgradeInProgress

Table 183: *tmnxChassisUpgradeInProgress* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2033 |
| Event name | tmnxChassisUpgradeInProgress |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.41 |
| Default severity | major |
| Source stream | main |
| Message format string | Class <i>\$tmnxHwClass\$</i> : 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 |

| Property name | Value |
|---------------|--|
| | 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. |

12.30 tmnxCpmALocalIcPortAvail

Table 184: 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 <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> 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 |

12.31 tmnxCpmANoLocalIcPort

Table 185: *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 <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> 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. |

12.32 tmnxCpmBLocalIcPortAvail

Table 186: *tmnxCpmBLocalIcPortAvail* properties

| Property name | Value |
|------------------|---------|
| Application name | CHASSIS |
| Event ID | 4010 |

| Property name | Value |
|----------------------------------|---|
| Event name | tmnxCpmBLocalcPortAvail |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.6 |
| Default severity | major |
| Source stream | main |
| Message format string | CPM <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> can reach the chassis using its local CPM interconnect ports |
| Cause | The tmnxCpmLocalcPortAvail 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 |

12.33 tmnxCpmBNoLocalcPort

Table 187: tmnxCpmBNoLocalcPort properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4008 |
| Event name | tmnxCpmBNoLocalcPort |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.5 |
| Default severity | major |
| Source stream | main |
| Message format string | CPM <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> can not reach the chassis using its local CPM interconnect ports |
| Cause | The tmnxCpmNoLocalcPort 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. |

| Property name | Value |
|---------------|--|
| | 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 tmnxCpmNoLocalCPort 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 tmnxCpmNoLocalCPort 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. |

12.34 tmnxCpmCardSyncFileNotPresent

Table 188: 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 |
| Source stream | main |
| Message format string | Class <i>\$tmnxHwClass\$</i> : Optional file <i>\$tmnxChassisNotifyCardSyncFile\$</i> 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 |

12.35 tmnxCpmlcPortDDMClear

Table 189: *tmnxCpmlcPortDDMClear* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 4016 |
| Event name | tmnxCpmlcPortDDMClear |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.9 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF DDM <i>\$tmnxDDMLaneIdOrModule\$ (\$tmnxDDMFailedObject\$)</i> cleared |
| Cause | The tmnxCpmlcPortDDMFailure 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 |

12.36 tmnxCpmlcPortDDMFailure

Table 190: *tmnxCpmlcPortDDMFailure* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 4015 |
| Event name | tmnxCpmlcPortDDMFailure |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.8 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF DDM <i>\$tmnxDDMLaneIdOrModule\$ (\$tmnxDDMFailedObject\$)</i> raised |

| Property name | Value |
|---------------|--|
| Cause | The <code>tmnxCpmlcPortDDMFailure</code> 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 |

12.37 `tmnxCpmlcPortDown`

Table 191: `tmnxCpmlcPortDown` properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 4003 |
| Event name | <code>tmnxCpmlcPortDown</code> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB. <code>tmnxCpmlcPortNotifications.1</code> |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port is not operational. Error code = <code>\$tmnxCpmlcPortOperState\$</code> |
| Cause | The <code>tmnxCpmlcPortDown</code> 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. |

12.38 `tmnxCpmlcPortSFFInserted`

Table 192: *tmnxCpmlcPortSFFInserted* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 4005 |
| Event name | tmnxCpmlcPortSFFInserted |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.3 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF inserted |
| Cause | The tmnxCpmlcPortSFFInserted 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 |

12.39 tmnxCpmlcPortSFFRemoved

Table 193: *tmnxCpmlcPortSFFRemoved* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4006 |
| Event name | tmnxCpmlcPortSFFRemoved |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.4 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port SFF removed |

| Property name | Value |
|---------------|---|
| Cause | The tmnxCpmlcPortSFFRemoved 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 tmnxCpmlcPortDown 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. |

12.40 tmnxCpmlcPortUp

Table 194: tmnxCpmlcPortUp properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4004 |
| Event name | tmnxCpmlcPortUp |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxCpmlcPort Notifications.2 |
| Default severity | minor |
| Source stream | main |
| Message format string | CPM interconnect port is operational |
| Cause | The tmnxCpmlcPortUp 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 |

12.41 tmnxCpmMemSizeMismatch

Table 195: *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 <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> has a different memory size than the active <i>\$tmnxChassisNotifyHwIndex\$</i> |
| 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. |

12.42 tmnxCpmMemSizeMismatchClear

Table 196: *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 <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> has the same memory size as the active <i>\$tmnxChassisNotifyHwIndex\$</i> |

| Property name | Value |
|---------------|--|
| Cause | A <code>tmnxCpmMemSizeMismatchClear</code> notification is generated when the RAM memory sizes of the standby (i.e., <code>tmnxChassisNotifyCpmCardSlotNum</code>) and active (i.e., <code>tmnxChassisNotifyHwIndex</code>) CPMs become matched. |
| Effect | The <code>tmnxCpmMemSizeMismatch</code> notification is cleared. |
| Recovery | There is no recovery required for this notification. |

12.43 `tmnxDcpCardFpEventOvrflw`

Table 197: `tmnxDcpCardFpEventOvrflw` properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2084 |
| Event name | <code>tmnxDcpCardFpEventOvrflw</code> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <code>tmnxChassisNotification.72</code> |
| Default severity | minor |
| Source stream | main |
| Message format string | TODO |
| Cause | The <code>tmnxDcpCardFpEventOvrflw</code> 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. |

12.44 `tmnxDcpCardFpEventOvrflwClr`

Table 198: *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. |

12.45 tmnxDcpCardSapEventOvrflw

Table 199: *tmnxDcpCardSapEventOvrflw* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2085 |
| Event name | tmnxDcpCardSapEventOvrflw |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.73 |
| Default severity | minor |
| 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 |

| Property name | Value |
|---------------|--|
| | 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. |

12.46 tmnxDcpCardSapEventOvrflwClr

Table 200: 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. |

12.47 tmnxDcpCardVrtrIfEventOvrflw

Table 201: tmnxDcpCardVrtrIfEventOvrflw properties

| Property name | Value |
|------------------|---------|
| Application name | CHASSIS |

| Property name | Value |
|----------------------------------|--|
| Event ID | 2086 |
| Event name | tmnxDcpCardVrtrlfEventOvrflw |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.74 |
| Default severity | minor |
| Source stream | main |
| Message format string | TODO |
| Cause | The tmnxDcpCardVrtrlfEventOvrflw 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. |

12.48 tmnxDcpCardVrtrlfEventOvrflwClr

Table 202: tmnxDcpCardVrtrlfEventOvrflwClr properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2091 |
| Event name | tmnxDcpCardVrtrlfEventOvrflwClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.79 |
| Default severity | minor |
| Source stream | main |
| Message format string | TODO |
| Cause | The tmnxDcpCardVrtrlfEventOvrflwClr 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. |

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

12.49 tmnxDcpFpDynPoolUsageHiAlmClear

Table 203: 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. |

12.50 tmnxDcpFpDynPoolUsageHiAlmRaise

Table 204: tmnxDcpFpDynPoolUsageHiAlmRaise properties

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

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.75 |
| Default severity | minor |
| 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. |

12.51 tmnxEnvTempTooHigh

Table 205: 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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$</i> : temperature too high |
| 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. |

12.52 tmnxEqBpEpromFail

Table 206: *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. |

12.53 tmnxEqBpEpromFailClear

Table 207: *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 |

| Property name | Value |
|-----------------------|---|
| 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 |

12.54 tmnxEqBpEpromWarning

Table 208: 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. |
| Recovery | No recovery action required. |

12.55 tmnxEqBpEpromWarningClear

Table 209: *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 |

12.56 tmnxEqCardChipIfCellEvent

Table 210: *tmnxEqCardChipIfCellEvent* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2103 |
| Event name | tmnxEqCardChipIfCellEvent |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.90 |
| Default severity | minor |
| Source stream | main |
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> experienced internal datapath cell errors • Slot <i>\$tmnxHwIndex\$</i> experienced internal datapath cell errors on complex <i>\$tmnxCardComplexNumber\$</i> |

| Property name | Value |
|---------------|---|
| 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. |

12.57 tmnxEqCardChipIfDownEvent

Table 211: 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: <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> experienced an internal datapath problem • Slot <i>\$tmnxHwIndex\$</i> experienced an internal datapath problem on complex <i>\$tmnxCardComplexNumber\$</i> |
| 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 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. |

12.58 tmnxEqCardFailure

Table 212: 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 <i>\$tmnxHwClass\$</i> : failed, reason: <i>\$tmnxChassisNotifyCardFailureReason\$</i> |
| 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 XMA 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. |

12.59 tmnxEqCardFirmwareUpgraded

Table 213: *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 <i>\$tmnxHwClass\$</i> : 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 |

12.60 tmnxEqCardInserted

Table 214: *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 <i>\$tmnxHwClass\$</i> : inserted |
| Cause | Generated when a card is inserted into the chassis. The card type may be IOM, Fabric, MDA, MCM, CCM CPM module, compact flash module, etc. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

12.61 tmnxEqCardMissing

Table 215: 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 <i>\$tmnxHwClass\$</i> : 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. |

12.62 tmnxEqCardMissingClear

Table 216: tmnxEqCardMissingClear properties

| Property name | Value |
|------------------|------------------------|
| Application name | CHASSIS |
| Event ID | 6008 |
| Event name | tmnxEqCardMissingClear |

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.304 |
| Default severity | cleared |
| Source stream | main |
| Message format string | Class <i>\$tmnxHwClass\$</i> : 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 |

12.63 tmnxEqCardPChipCamEvent

Table 217: *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 <i>\$tmnxSlotNum\$</i> -forwarding engine <i>\$tmnxCardComplexNumber\$</i> |
| Cause | The tmnxEqCardPChipCamEvent notification is generated when either an IOM or a CPM experiences a persistent occurrence of a PChip CAM error. On a CPM card, the tmnxCardComplexNumber will be fixed to the value zero (0). |
| Effect | Contact Nokia customer support. |
| Recovery | Contact Nokia customer support. |

12.64 tmnxEqCardPChipError

Table 218: 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 <i>\$tmnxCardSlotNum\$</i> detected <i>\$tmnxCardFwdDirection\$</i> FCS errors on complex <i>\$tmnxCardComplexNumber\$</i> . Source card(s) of detected errors: <i>\$tmnxCardSrcSlotBitmap\$</i> |
| 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 |

12.65 tmnxEqCardPChipMemoryEvent

Table 219: 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 |

| Property name | Value |
|-----------------------|--|
| Source stream | main |
| Message format string | Possible messages: <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> experienced a pchip memory error occurrence • Slot <i>\$tmnxHwIndex\$</i> experienced a pchip parity error occurrence on complex <i>\$tmnxCardComplexNumber\$</i> |
| Cause | The tmnxEqCardPChipMemoryEvent notification is generated when a P-chip experiences an occurrence of a memory error. |
| Effect | N/A |
| Recovery | N/A |

12.66 tmnxEqCardQChipBufMemoryEvent

Table 220: 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: <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> experienced a Q-chip buffer memory error occurrence • Slot <i>\$tmnxHwIndex\$</i> experienced a Q-chip buffer memory error occurrence on complex <i>\$tmnxCardComplexNumber\$</i> |
| 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. |

12.67 tmnxEqCardQChipIntMemoryEvent

Table 221: *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: <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> experienced a qchip internal memory error occurrence • Slot <i>\$tmnxHwIndex\$</i> experienced a qchip internal memory error occurrence on complex <i>\$tmnxCardComplexNumber\$</i> |
| 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. |

12.68 tmnxEqCardQChipStatsMemoryEvent

Table 222: *tmnxEqCardQChipStatsMemoryEvent* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2099 |
| Event name | tmnxEqCardQChipStatsMemoryEvent |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.87 |

| Property name | Value |
|-----------------------|--|
| Default severity | minor |
| Source stream | main |
| Message format string | Possible messages: <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> experienced a Q-chip statistics memory error occurrence • Slot <i>\$tmnxHwIndex\$</i> experienced a Q-chip statistics memory error occurrence on complex <i>\$tmnxCardComplexNumber\$</i> |
| 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. |

12.69 tmnxEqCardRemoved

Table 223: *tmnxEqCardRemoved* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2003 |
| Event name | tmnxEqCardRemoved |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.9 |
| Default severity | major |
| Source stream | main |
| Message format string | Class <i>\$tmnxHwClass\$</i> : 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. |

| Property name | Value |
|---------------|--|
| 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. |

12.70 tmnxEqCardSoftResetAlarm

Table 224: 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 <i>\$tmnxHwIndex\$</i> entered soft-reset state <i>\$tmnxCardSoftResetState\$</i> |
| Cause | The tmnxEqCardSoftResetAlarm notification is generated when an IOM card enters and exits the 'soft-reset' state. |
| Effect | N/A |
| Recovery | N/A |

12.71 tmnxEqCardTChipParityEvent

Table 225: tmnxEqCardTChipParityEvent properties

| Property name | Value |
|------------------|----------------------------|
| Application name | CHASSIS |
| Event ID | 2110 |
| Event name | tmnxEqCardTChipParityEvent |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.97 |
| Default severity | minor |
| Source stream | main |
| Message format string | Slot <i>\$tmnxHwIndex\$</i> experienced a T-chip memory error occurrence on complex <i>\$tmnxCardComplexNumber\$</i> |
| 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. |

12.72 tmnxEqDataPathFailureProtImpact

Table 226: *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 |
| Message format string | <i>\$tmnxHwClass\$ \$tmnxHwIndex\$</i> 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 |

12.73 tmnxEqEsaHostPortCrcAlarm

Table 227: *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 <i>\$tmnxEsaHostPortNotifCrcAlrm Value\$</i> threshold <i>\$tmnxEsaHostPortNotifCrcMltiplier\$*10e-\$tmnxEsaHostPortNotifCrcThreshold\$</i> 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. |

12.74 tmnxEqEsaHostPortCrcAlarmClear

Table 228: *tmnxEqEsaHostPortCrcAlarmClear* properties

| Property name | Value |
|------------------|--------------------------------|
| Application name | CHASSIS |
| Event ID | 6010 |
| Event name | tmnxEqEsaHostPortCrcAlarmClear |

| Property name | Value |
|----------------------------------|--|
| 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 <i>\$tmnxEsaHostPortNotifCrcAlm Value\$</i> threshold <i>\$tmnxEsaHostPortNotifCrcMltiplier\$</i> *10e- <i>\$tmnxEsaHostPortNotifCrcThreshold\$</i> Cleared |
| Cause | The tmnxEqEsaHostPortCrcAlarmClear is generated when an Ethernet port CRC alarm condition is cleared or disabled. |
| Effect | N/A |
| Recovery | N/A |

12.75 tmnxEqFlashDataLoss

Table 229: 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 |
| Message format string | Class <i>\$tmnxHwClass\$</i> : 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 |

12.76 tmnxEqFlashDiskFull

Table 230: *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 <i>\$tmnxHwClass\$</i> : <i>\$tmnxChassisNotifyDiskFullReason\$</i> |
| 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 |

12.77 tmnxEqFpgaSoftError

Table 231: *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 <i>\$tmnxHwIndex\$</i> detected an SEU event |

| Property name | Value |
|---------------|--|
| 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. |

12.78 tmnxEqHwEnhancedCapability

Table 232: 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 <i>\$tmnxCardSlotNum\$</i> has enhanced capabilities. |
| Cause | The tmnxEqHwEnhancedCapability notification is generated when the hardware, specified by the supplied objects, consists of enhanced capabilities as compared to the active hardware. |
| Effect | The system behaves normally under this situation, however, switching to the newer hardware will put the system in an incompatible state with the currently active hardware. That is, once this device takes activity, the lesser capable hardware will fail to communicate with it. In this mode, the system is deemed in a 'one-way upgrade' scenario. |
| Recovery | Two modes of recovery exist for this notification: 1) Remove the enhanced hardware, and supply a more compatible device (status quo) with the active hardware. 2) Switch to the enhanced device, and replace the older hardware with a similarly enhanced device (upgrade). |

12.79 tmnxEqHwEventDetected

Table 233: *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 | <i>\$tmnxHwClass\$ \$tmnxChassisNotifyHwIndex\$: \$tmnxEqNotifyHwEventType\$ event detected. (detail: \$tmnxEqNotifyHwEventDetail\$, action: \$tmnxEqNotifyHwEventAction\$)</i> |
| 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. |

12.80 tmnxEqLowPowerSwFabModeDisabled

Table 234: *tmnxEqLowPowerSwFabModeDisabled* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 6017 |
| Event name | tmnxEqLowPowerSwFabModeDisabled |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.314 |
| Default severity | minor |

| Property name | Value |
|-----------------------|---|
| Source stream | main |
| Message format string | Low power switch fabric mode is disabled |
| Cause | The tmnxEqLowPowerSwFabModeDisabled event is generated when low power switch fabric mode is disabled. |
| Effect | SFMs are operational and the switch fabric is at full capacity. |
| Recovery | N/A |

12.81 tmnxEqLowPowerSwFabModeEnabled

Table 235: tmnxEqLowPowerSwFabModeEnabled properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 6016 |
| Event name | tmnxEqLowPowerSwFabModeEnabled |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.313 |
| Default severity | minor |
| Source stream | main |
| Message format string | Low power switch fabric mode is enabled |
| Cause | The tmnxEqLowPowerSwFabModeEnabled event is generated when low power switch fabric mode is enabled. |
| Effect | SFMs are in power save mode and the switch fabric operates at a reduced capacity to save power. |
| Recovery | Disable the low power switch fabric mode configuration. |

12.82 tmnxEqLowSwitchFabricCap

Table 236: *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 <i>\$tmnxHwClass\$ \$tmnxHwIndex\$</i> 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. |

12.83 tmnxEqLowSwitchFabricCapClear

Table 237: *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 |
| Source stream | main |
| Message format string | The switch fabric capacity alarm for <i>\$tmnxHwClass\$ \$tmnxHwIndex\$</i> was cleared. |

| Property name | Value |
|---------------|---|
| 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 |

12.84 tmnxEqMdaCfgNotCompatible

Table 238: 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 <i>\$tmnxHwClass\$</i> : 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. |

12.85 tmnxEqMdaIngrXplError

Table 239: *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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxEqMdaSlotNum\$</i> 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. |

12.86 tmnxEqMdaSyncENotCompatible

Table 240: *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 |
| 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 |

| Property name | Value |
|---------------|--|
| | 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. |

12.87 tmnxEqMdaXplError

Table 241: 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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxMDASlotNum\$</i> 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 |

12.88 tmnxEqMgmtEthRedStandbyClear

Table 242: *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 <i>\$tmnxChassisNotifyMgmtEthRedPort\$</i> is serving as the system's management Ethernet port. |
| Cause | The <i>tmnxEqMgmtEthRedStandbyClear</i> 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. |

12.89 tmnxEqMgmtEthRedStandbyRaise

Table 243: *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 <i>\$tmnxChassisNotifyMgmtEthRedPort\$</i> is serving as the system's management Ethernet port. |
| Cause | The <i>tmnxEqMgmtEthRedStandbyRaise</i> 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. |

12.90 tmnxEqOperStateChange

Table 244: *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 | <i>\$tmnxNotifyObjectName\$</i> changed operational state: <i>\$tmnxNotifyRowOperState\$</i> |
| Cause | The <i>tmnxEqOperStateChange</i> 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. |

12.91 tmnxEqPhysChassisFanFailure

Table 245: *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 <i>\$tmnxPhysChassisNum\$</i> fan <i>\$tmnxPhysChassisFanIndex\$</i> 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. |

12.92 tmnxEqPhysChassisFanFailureClear

Table 246: *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 <i>\$tmnxPhysChassisNum\$</i> fan <i>\$tmnxPhysChassisFanIndex\$</i> failure cleared |
| Cause | The <i>tmnxEqPhysChassisFanFailureClear</i> 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. |

12.93 *tmnxEqPhysChassPowerSupAcFail*

Table 247: *tmnxEqPhysChassPowerSupAcFail* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2140 |
| Event name | <i>tmnxEqPhysChassPowerSupAcFail</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.127</i> |
| Default severity | critical |
| Source stream | main |
| Message format string | Chassis <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupld\$</i> AC failure |
| Cause | The <i>tmnxEqPhysChassPowerSupAcFail</i> 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. |

12.94 *tmnxEqPhysChassPowerSupAcFailClr*

Table 248: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChass PowerSupld\$</i> 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. |

12.95 tmnxEqPhysChassPowerSupDcFail

Table 249: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChass PowerSupld\$</i> 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. |

12.96 tmnxEqPhysChassPowerSupDcFailClr

Table 250: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChass PowerSupId\$</i> 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. |

12.97 tmnxEqPhysChassPowerSupInFail

Table 251: *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 PowerSupld\$ 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. |

12.98 tmnxEqPhysChassPowerSupInFailClr

Table 252: 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 PowerSupld\$ 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. |

12.99 tmnxEqPhysChassPowerSupOutFail

Table 253: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupId\$</i> 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. |

12.100 tmnxEqPhysChassPowerSupOutFailCl

Table 254: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChass PowerSupld\$</i> 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. |

12.101 tmnxEqPhysChassPowerSupOvrTmp

Table 255: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChass PowerSupld\$</i> 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. |

12.102 tmnxEqPhysChassPowerSupOvrTmpClr

Table 256: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChass PowerSupId\$</i> 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. |

12.103 tmnxEqPowerCapacityExceeded

Table 257: *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 <i>\$tmnxChassisNotify PowerCapacity\$</i> 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. |

12.104 tmnxEqPowerCapacityExceededClear

Table 258: 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 |

12.105 tmnxEqPowerLostCapacity

Table 259: *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 <i>\$tmnxChassisNotifyPowerCapacity\$</i> 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. |

12.106 tmnxEqPowerLostCapacityClear

Table 260: *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 |

12.107 tmnxEqPowerOverloadState

Table 261: 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. |

12.108 tmnxEqPowerOverloadStateClear

Table 262: *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 |

12.109 tmnxEqPowerSafetyAlertClear

Table 263: *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: <ul style="list-style-type: none"> The system power capacity safety alert for zone <i>\$tmnxChassisPwr MgmtZone\$</i> has been disabled. |

| Property name | Value |
|---------------|--|
| | <ul style="list-style-type: none"> The system power capacity for zone <i>\$tmnxChassisPwrMgmtZone\$</i> meets or exceeds the configured safety alert threshold of <i>\$tmnxChassisPwrMgmtSafetyAlert\$</i> 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 |

12.110 tmnxEqPowerSafetyAlertThreshold

Table 264: 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 <i>\$tmnxChassisPwrMgmtZone\$</i> dropped below the configured safety alert threshold of <i>\$tmnxChassisPwrMgmtSafetyAlert\$</i> 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 |

12.111 tmnxEqPowerSafetyLevelClear

Table 265: *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 <i>\$tmnxChassisPwrMgmtZone\$</i> consumption dropped below the configured safety level threshold of <i>\$tmnxChassisPwrMgmtSafetyLevel\$</i> 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 |

12.112 tmnxEqPowerSafetyLevelThreshold

Table 266: *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 <i>\$tmnxChassisPwrMgmtZone\$</i> consumption exceeded the configured safety level threshold of <i>\$tmnxChassisPwrMgmtSafetyLevel\$</i> 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 |

12.113 tmnxEqPowerSupplyInserted

Table 267: 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 | <i>\$tmnxChassisNotifyHwIndex\$</i> inserted |
| Cause | Generated when one of the chassis' power supplies is inserted. |
| Effect | N/A |
| Recovery | N/A |

12.114 tmnxEqPowerSupplyRemoved

Table 268: 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 | <i>\$tmnxChassisNotifyHwIndex\$, power lost</i> |
| 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. |

12.115 tmnxEqProvPowerCapacityAlm

Table 269: 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. |

12.116 tmnxEqProvPowerCapacityAlmClr

Table 270: 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 |

12.117 tmnxEqSynclftimingBITS2Alarm

Table 271: tmnxEqSynclftimingBITS2Alarm properties

| Property name | Value |
|------------------|------------------------------|
| Application name | CHASSIS |
| Event ID | 2073 |
| Event name | tmnxEqSynclftimingBITS2Alarm |

| 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 <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.118 tmnxEqSynclfTimingBITS2AlarmClr

Table 272: *tmnxEqSynclfTimingBITS2AlarmClr* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2074 |
| Event name | tmnxEqSynclfTimingBITS2AlarmClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.62 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.119 tmnxEqSynclfTimingBITS2Quality

Table 273: *tmnxEqSynclfTimingBITS2Quality* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2071 |
| Event name | tmnxEqSynclfTimingBITS2Quality |
| 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 <i>\$tmnxSynclfTimingBITS2RxQtyLevel\$</i> |
| Cause | Generated when there is a change of the received quality level on the second bits interface. |
| Effect | N/A |
| Recovery | N/A |

12.120 tmnxEqSynclfTimingBITSAalarm

Table 274: *tmnxEqSynclfTimingBITSAalarm* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2030 |
| Event name | tmnxEqSynclfTimingBITSAalarm |
| 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 <i>\$tmnxSynclfTimingNotifyAlarm\$</i> on BITS <i>\$bits-two-supported\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.121 tmnxEqSynclfTimingBITSAAlarmClear

Table 275: *tmnxEqSynclfTimingBITSAAlarmClear* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2031 |
| Event name | <i>tmnxEqSynclfTimingBITSAAlarmClear</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.39</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclfTimingNotifyAlarm\$</i> on BITS <i>\$bits-two-supported\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.122 tmnxEqSynclfTimingBITSOOutRefChg

Table 276: *tmnxEqSyncIfTimingBITSOOutRefChg* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2075 |
| Event name | tmnxEqSyncIfTimingBITSOOutRefChg |
| 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 <i>\$tmnxSyncIfTimingBITSOOutRefSel\$</i> |
| Cause | Generated when the BITS Out timing reference selection changes. |
| Effect | N/A |
| Recovery | N/A |

12.123 tmnxEqSyncIfTimingBITSQuality

Table 277: *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 <i>\$bits-two-supported\$</i> received quality level <i>\$tmnxSyncIfTimingBITSRxQtyLevel\$</i> |
| 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 |

12.124 tmnxEqSyncIfTimingGnss2Alarm

Table 278: 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 <i>\$tmnxSyncIfTimingNotifyAlarm\$</i> 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 tmnxSyncIfTimingNotifyAlarm 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. |

12.125 tmnxEqSyncIfTimingGnss2AlarmClr

Table 279: tmnxEqSyncIfTimingGnss2AlarmClr properties

| Property name | Value |
|------------------|---------|
| Application name | CHASSIS |

| Property name | Value |
|----------------------------------|--|
| Event ID | 2229 |
| Event name | tmnxEqSynclfTimingGnss2AlarmClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.240 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 |

12.126 tmnxEqSynclfTimingGnss2Quality

Table 280: *tmnxEqSynclfTimingGnss2Quality* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2225 |
| Event name | tmnxEqSynclfTimingGnss2Quality |
| 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 <i>\$tmnxSynclfTimingGnss2RxQtyLevel\$</i> |
| Cause | Generated when there is a change of the received quality level on timing reference gnss2. |
| Effect | N/A |
| Recovery | N/A |

12.127 tmnxEqSyncIftimingGnssAlarm

Table 281: *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 <i>\$tmnxSyncIftimingNotifyAlarm\$</i> 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 tmnxSyncIftimingNotifyAlarm 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. |

12.128 tmnxEqSyncIftimingGnssAlarmClr

Table 282: *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 <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.129 tmnxEqSynclfTimingGnssQuality

Table 283: *tmnxEqSynclfTimingGnssQuality* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2224 |
| Event name | tmnxEqSynclfTimingGnssQuality |
| 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 <i>\$tmnxSynclfTimingGnssRxQltyLevel\$</i> |
| Cause | Generated when there is a change of the received quality level on timing reference gnss. |
| Effect | N/A |
| Recovery | N/A |

12.130 tmnxEqSynclfTimingHoldover

Table 284: *tmnxEqSyncIftTimingHoldover* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2017 |
| Event name | tmnxEqSyncIftTimingHoldover |
| 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. |

12.131 tmnxEqSyncIftTimingHoldoverClear

Table 285: *tmnxEqSyncIftTimingHoldoverClear* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2018 |
| Event name | tmnxEqSyncIftTimingHoldoverClear |
| 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 tmnCpmCardTable. |
| Effect | N/A |
| Recovery | N/A |

12.132 tmnxEqSyncIfTimingPTPAlarm

Table 286: 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 <i>\$tmnxSyncIfTimingNotifyAlarm\$</i> 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 tmnCpmCardTable. |
| Effect | N/A |
| Recovery | N/A |

12.133 tmnxEqSyncIfTimingPTPAlarmClr

Table 287: *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 <i>\$tmnxSyncIfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.134 tmnxEqSyncIfTimingPTPQuality

Table 288: *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 <i>\$tmnxSyncIfTimingPTPRxQtyLevel\$</i> |

| 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 |

12.135 tmnxEqSyncIftTimingRef1Alarm

Table 289: tmnxEqSyncIftTimingRef1Alarm properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2019 |
| Event name | tmnxEqSyncIftTimingRef1Alarm |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.28 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSyncIftTimingNotifyAlarm\$</i> 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 tmnxSyncIftTimingNotifyAlarm 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). |

12.136 tmnxEqSyncIftTimingRef1AlarmClear

Table 290: *tmnxEqSyncIftTimingRef1AlarmClear* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2020 |
| Event name | tmnxEqSyncIftTimingRef1AlarmClear |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.29 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSyncIftTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.137 tmnxEqSyncIftTimingRef1Quality

Table 291: *tmnxEqSyncIftTimingRef1Quality* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2068 |
| Event name | tmnxEqSyncIftTimingRef1Quality |
| 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 <i>\$tmnxSyncIftTimingRef1RxQtyLevel\$</i> |

| 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 |

12.138 tmnxEqSynclftimingRef2Alarm

Table 292: *tmnxEqSynclftimingRef2Alarm* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2021 |
| Event name | tmnxEqSynclftimingRef2Alarm |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.30 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclftimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.139 tmnxEqSynclftimingRef2AlarmClear

Table 293: *tmnxEqSynclftimingRef2AlarmClear* properties

| Property name | Value |
|------------------|---------|
| Application name | CHASSIS |

| Property name | Value |
|----------------------------------|---|
| Event ID | 2022 |
| Event name | tmnxEqSynclfTimingRef2AlarmClear |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.31 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.140 tmnxEqSynclfTimingRef2Quality

Table 294: *tmnxEqSynclfTimingRef2Quality* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2069 |
| Event name | tmnxEqSynclfTimingRef2Quality |
| 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 <i>\$tmnxSynclfTimingRef2RxQtyLevel\$</i> |
| Cause | Generated when there is a change of the received quality level on timing reference 2. |
| Effect | N/A |
| Recovery | N/A |

12.141 tmnxEqSyncIfTimingRefSwitch

Table 295: *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 <i>\$tmnxSyncIfTimingRef1InUse\$</i> |
| Cause | Generated when there is a change of which timing reference is providing timing for the system. |
| Effect | N/A |
| Recovery | N/A |

12.142 tmnxEqSyncIfTimingSyncE2Alarm

Table 296: *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 <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.143 tmnxEqSynclfTimingSyncE2AlarmClr

Table 297: *tmnxEqSynclfTimingSyncE2AlarmClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2206 |
| Event name | <i>tmnxEqSynclfTimingSyncE2AlarmClr</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.217</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 <i>tmnxCpmCardTable</i> . |
| Effect | N/A |
| Recovery | N/A |

12.144 tmnxEqSynclfTimingSyncE2Quality

Table 298: *tmnxEqSynclfTimingSyncE2Quality* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2202 |
| Event name | tmnxEqSynclfTimingSyncE2Quality |
| 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 <i>\$tmnxSynclfTimingSyncE2RxQltyLevl\$</i> |
| Cause | Generated when there is a change of the received quality level on timing reference syncce2. |
| Effect | N/A |
| Recovery | N/A |

12.145 tmnxEqSynclfTimingSyncEAlarm

Table 299: *tmnxEqSynclfTimingSyncEAlarm* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2203 |
| Event name | tmnxEqSynclfTimingSyncEAlarm |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.214 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclfTimingNotifyAlarm\$</i> 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 tmnCpmCardTable. |
| Effect | N/A |
| Recovery | N/A |

12.146 tmnxEqSynclftimingSyncEAlarmClr

Table 300: tmnxEqSynclftimingSyncEAlarmClr properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2204 |
| Event name | tmnxEqSynclftimingSyncEAlarmClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.215 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous Timing interface, alarm <i>\$tmnxSynclftimingNotifyAlarm\$</i> 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 tmnCpmCardTable. |
| Effect | N/A |
| Recovery | N/A |

12.147 tmnxEqSynclftimingSyncEQuality

Table 301: *tmnxEqSynclftimingSyncEQuality* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2201 |
| Event name | tmnxEqSynclftimingSyncEQuality |
| 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 <i>\$tmnxSynclftimingSyncERxQtyLevel\$</i> |
| Cause | Generated when there is a change of the received quality level on timing reference syncce. |
| Effect | N/A |
| Recovery | N/A |

12.148 tmnxEqSynclftimingSystemQuality

Table 302: *tmnxEqSynclftimingSystemQuality* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2077 |
| Event name | tmnxEqSynclftimingSystemQuality |
| 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 <i>\$tmnxSynclftimingSystemQtyLevel\$</i> |
| 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. |

12.149 tmnxEqWrongCard

Table 303: *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 <i>\$tmnxHwClass\$</i> : 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. |

12.150 tmnxEsaCleared

Table 304: 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 |

12.151 tmnxEsaConnected

Table 305: 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 <i>\$tmnxEsaNotifyId\$</i> connected |
| Cause | The tmnxEsaConnected notification is generated when a new ESA is connected. |
| Effect | N/A |
| Recovery | N/A |

12.152 tmnxEsaDisconnected

Table 306: *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 <i>\$tmnxEsaNotifyId\$</i> disconnected |
| Cause | The tmnxEsaDisconnected notification is generated when an ESA is disconnected. |
| Effect | N/A |
| Recovery | N/A |

12.153 tmnxEsaDiscovered

Table 307: *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 <i>\$tmnxEsaNotifyId\$</i> discovered |
| Cause | The tmnxEsaDiscovered notification is generated when a new ESA is discovered by the system. |
| Effect | N/A |
| Recovery | N/A |

12.154 tmnxEsaFailure

Table 308: *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 <i>\$tmnxEsaNotifyId\$</i> failed with reason <i>\$tmnxEsaStatsOperFlags\$</i> |
| Cause | The tmnxEsaFailure notification is generated when a failure occurs on an ESA. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

12.155 tmnxEsaFirmwareUpgradeDone

Table 309: *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 <i>\$tmnxEsaNotifyId\$</i> Firmware upgrade done - <i>\$firmwareUpgradeStage\$</i> |
| Cause | The tmnxEsaFirmwareUpgradeInProgress notification is generated to indicate whenever a certain upgrade stage/device is complete. |
| Effect | N/A |
| Recovery | N/A |

12.156 tmnxEsaFirmwareUpgradeFailed

Table 310: *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 <i>\$tmnxEsaNotifyId\$</i> Firmware upgrade failed - <i>\$firmwareUpgradeStage\$</i> |
| 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. |

12.157 tmnxEsaFirmwareUpgradeInProgress

Table 311: 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 <i>\$tmnxEsaNotifyId\$</i> Firmware upgrade in progress - <i>\$firmwareUpgradeStage\$</i> |
| Cause | The tmnxEsaFirmwareUpgradeInProgress notification is generated to indicate the different upgrade stages/devices and the expected ESA reboots. |
| Effect | N/A |
| Recovery | N/A |

12.158 tmnxEsaFirmwareUpgradeStarted

Table 312: *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 <i>\$tmnxEsaNotifyId\$</i> 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 |

12.159 tmnxEsaHwFanBankFailRedun

Table 313: *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 <i>\$tmnxHwClass\$</i> 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. |

12.160 tmnxEsaHwFanBankFailRedunClr

Table 314: 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 |

12.161 tmnxEsaHwFanBankNonRedun

Table 315: 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. |

12.162 tmnxEsaHwFanBankNonRedunClr

Table 316: 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 |

12.163 tmnxEsaHwFanStatusDegraded

Table 317: *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 <i>\$tmnxHwClass\$</i> 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. |

12.164 tmnxEsaHwFanStatusDegradedClr

Table 318: *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 <i>\$tmnxHwClass\$</i> fan degraded status cleared, now <i>\$tmnxEsaStats FanStatus\$</i> |

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

12.165 tmnxEsaHwFanStatusFailed

Table 319: 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. |

12.166 tmnxEsaHwFanStatusFailedClr

Table 320: 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 \$tmnxEsaStatsFan Status\$ |
| Cause | The tmnxEsaHwFanStatusFailedClr notification is generated when the ESA fans are restored. |
| Effect | N/A |
| Recovery | N/A |

12.167 tmnxEsaHwPwrSup1Degraded

Table 321: 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. |

12.168 tmnxEsaHwPwrSup1DegradedClr

Table 322: *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 <i>\$tmnxHwClass\$</i> power supply 1 degraded status cleared, now <i>\$tmnxEsaStatsPowerSupply1Status\$</i> |
| Cause | The tmnxEsaHwPwrSup1DegradedClr notification is generated when the ESA power supply 1 is no longer degraded. |
| Effect | N/A |
| Recovery | N/A |

12.169 tmnxEsaHwPwrSup1Failed

Table 323: *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 <i>\$tmnxHwClass\$</i> 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. |

12.170 tmnxEsaHwPwrSup1FailedClr

Table 324: 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 <i>\$tmnxHwClass\$</i> power supply 1 failed status cleared, now <i>\$tmnxEsaStatsPowerSupply1Status\$</i> |
| Cause | The tmnxEsaHwPwrSup1FailedClr notification is generated when the ESA power supply 1 is restored. |
| Effect | N/A |
| Recovery | N/A |

12.171 tmnxEsaHwPwrSup2Degraded

Table 325: 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. |

12.172 tmnxEsaHwPwrSup2DegradedClr

Table 326: 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 |

12.173 tmnxEsaHwPwrSup2Failed

Table 327: *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. |

12.174 tmnxEsaHwPwrSup2FailedClr

Table 328: *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 <i>\$tmnxHwClass\$</i> power supply 2 failed status cleared, now <i>\$tmnxEsaStatsPowerSupply2Status\$</i> |
| Cause | The <i>tmnxEsaHwPwrSup2FailedClr</i> notification is generated when the ESA power supply 2 is restored. |
| Effect | N/A |
| Recovery | N/A |

12.175 *tmnxEsaHwPwrSupBankFailRedun*

Table 329: *tmnxEsaHwPwrSupBankFailRedun* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2424 |
| Event name | <i>tmnxEsaHwPwrSupBankFailRedun</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.289</i> |
| Default severity | critical |
| Source stream | main |
| Message format string | ESA <i>\$tmnxHwClass\$</i> power supply bank status failed-redundant |
| Cause | The <i>tmnxEsaHwPwrSupBankFailRedun</i> 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. |

12.176 *tmnxEsaHwPwrSupBankFailRedunClr*

Table 330: *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 <i>\$tmnxHwClass\$</i> power supply bank failed-redundant status cleared, now <i>\$tmnxEsaStatsPwrSupRedundancy\$</i> |
| Cause | The tmnxEsaHwPwrSupBankFailRedunClr notification is generated when the ESA power supplies regain redundancy. |
| Effect | N/A |
| Recovery | N/A |

12.177 tmnxEsaHwPwrSupBankNonRedun

Table 331: *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 <i>\$tmnxHwClass\$</i> 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. |

12.178 tmnxEsaHwPwrSupBankNonRedunClr

Table 332: *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 <i>\$tmnxHwClass\$</i> power supply bank non-redundant status cleared, now <i>\$tmnxEsaStatsPwrSupRedundancy\$</i> |
| Cause | The tmnxEsaHwPwrSupBankNonRedunClr notification is generated when the ESA power supplies return to a fully redundant state. |
| Effect | N/A |
| Recovery | N/A |

12.179 tmnxEsaHwPwrSupMismatch

Table 333: *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 <i>\$tmnxHwClass\$</i> power supply mismatch |
| Cause | The <i>tmnxEsaHwPwrSupMismatch</i> 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. |

12.180 *tmnxEsaHwPwrSupMismatchClr*

Table 334: *tmnxEsaHwPwrSupMismatchClr* properties

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

12.181 *tmnxEsaHwStatusCritical*

Table 335: *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 <i>\$tmnxHwClass\$</i> 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. |

12.182 tmnxEsaHwStatusCriticalClr

Table 336: *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 <i>\$tmnxHwClass\$</i> aggregate hardware status critical - cleared, now <i>\$tmnxEsaStatsHardwareStatus\$</i> |
| Cause | The tmnxEsaHwStatusCriticalClr notification is generated when the ESA hardware status is no longer critical. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

12.183 tmnxEsaHwStatusDegraded

Table 337: *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. |

12.184 tmnxEsaHwStatusDegradedClr

Table 338: *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 <i>\$tmnxHwClass\$</i> aggregate hardware degraded status cleared, now <i>\$tmnxEsaStatsHardwareStatus\$</i> |
| Cause | The <i>tmnxEsaHwStatusDegradedClr</i> notification is generated when ESA hardware components are no longer degraded. |
| Effect | N/A |
| Recovery | N/A |

12.185 *tmnxEsaHwTemperatureDegraded*

Table 339: *tmnxEsaHwTemperatureDegraded* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2426 |
| Event name | <i>tmnxEsaHwTemperatureDegraded</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.291</i> |
| Default severity | critical |
| Source stream | main |
| Message format string | ESA <i>\$tmnxHwClass\$</i> temperature status degraded |
| Cause | The <i>tmnxEsaHwTemperatureDegraded</i> 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. |

12.186 *tmnxEsaHwTemperatureDegradedClr*

Table 340: *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 <i>\$tmnxHwClass\$</i> temperature degraded status cleared, now <i>\$tmnxEsaStatsTemperatureStatus\$</i> |
| Cause | The <i>tmnxEsaHwTemperatureDegradedClr</i> notification is generated when the ESA returns to a temperature within the expected operating range. |
| Effect | N/A |
| Recovery | N/A |

12.187 *tmnxEsaHwTemperatureFailed*

Table 341: *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 <i>\$tmnxHwClass\$</i> temperature status failed |
| Cause | The <i>tmnxEsaHwTemperatureFailed</i> 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. |

12.188 tmnxEsaHwTemperatureFailedClr

Table 342: *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 <i>\$tmnxHwClass\$</i> temperature failed status cleared, now <i>\$tmnxEsaStatsTemperatureStatus\$</i> |
| Cause | The tmnxEsaHwTemperatureFailedClr notification is generated when the ESA returns to a temperature within the expected operating range. |
| Effect | N/A |
| Recovery | N/A |

12.189 tmnxEsaStolenTimeDetected

Table 343: *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. |

12.190 tmnxEsaVmBooted

Table 344: 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 |

12.191 tmnxEsaVmCleared

Table 345: *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 <i>\$tmnxEsaNotifyId\$</i> / <i>\$tmnxEsaVmNotifyId\$</i> reset |
| Cause | The tmnxEsaVmCleared notification is generated when an ESA VM is cleared or restarted. |
| Effect | N/A |
| Recovery | N/A |

12.192 tmnxEsaVmCreated

Table 346: *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 <i>\$tmnxEsaNotifyId\$</i> / <i>\$tmnxEsaVmNotifyId\$</i> created |

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

12.193 tmnxEsaVmFailure

Table 347: 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 <i>\$tmnxEsaNotifyId\$</i> / <i>\$tmnxEsaVmNotifyId\$</i> failed with reason <i>\$tmnxEsaVmStatsOperFlags\$</i> |
| Cause | The tmnxEsaVmFailure notification is generated when an ESA VM crashes. |
| Effect | N/A |
| Recovery | N/A |

12.194 tmnxEsaVmRemoved

Table 348: 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 <i>\$tmnxEsaNotifyId\$/\$tmnxEsaVmNotifyId\$</i> destroyed |
| Cause | The tmnxEsaVmRemoved notification is generated when an ESA VM is removed. |
| Effect | N/A |
| Recovery | N/A |

12.195 tmnxExtStandbyCpmReboot

Table 349: *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. |

12.196 tmnxExtStandbyCpmRebootFail

Table 350: *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. |

12.197 tmnxFPResourcePolicyModified

Table 351: *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 <i>\$tmnxHwClass\$</i> : 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. |

12.198 tmnxFPResourcePolicyModifiedClr

Table 352: *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 <i>\$tmnxHwClass\$</i> : Card : alarm <i>\$tmnxFPResourcePolicyModified</i> \$ cleared |

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

12.199 tmnxFPResOversubscribed

Table 353: 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 congestion on the system. More specific action might be required depending on the specific oversubscription. |

12.200 tmnxFPResOversubscribedCleared

Table 354: *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. |

12.201 tmnxGnssAcquiredFix

Table 355: *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 |

12.202 tmnxGnssAcquiringFix

Table 356: *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. |

12.203 tmnxHwAggShpSchedEventOvrflw

Table 357: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxHwAggShpTimeEventOccured\$</i> |
| 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. |

12.204 tmnxHwAggShpSchedEventOvrflwClr

Table 358: 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 | <i>\$tmnxHwAggShpMissingNotifCount\$</i> HW Agg Shaper Sched events were dropped in the last event throttling interval on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxHwAggShpTimeEventOccured\$</i> |
| 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. |

12.205 tmnxInterChassisCommsDown

Table 359: *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. |

12.206 tmnxInterChassisCommsUp

Table 360: *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.tmnxInterChassisNotifications.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 |

12.207 tmnxlomEventOverflow

Table 361: tmnxlomEventOverflow properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2124 |
| Event name | tmnxlomEventOverflow |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.111 |
| Default severity | minor |
| Source stream | main |
| Message format string | lom <i>\$tmnxlomResourceType\$</i> Resource event overflow occurred on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxlomResLimitTimeEventOccured\$</i> . |
| Cause | The tmnxlomEventOverflow notification is generated when tmnxlomResStateClr, tmnxlomResExhausted and tmnxlomResHighLimit 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. |

12.208 tmnxlomEventOverflowClr

Table 362: tmnxlomEventOverflowClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2125 |
| Event name | tmnxlomEventOverflowClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.112 |
| Default severity | minor |
| Source stream | main |
| Message format string | <i>\$tmnxlomResLimMissingNotifCount\$ lom \$tmnxlomResourceType \$ Resources events were dropped in the last event throttling interval on card \$tmnxChassisNotifyCardSlotNum\$ at \$tmnxlomResLimitTime EventOccured\$.</i> |
| Cause | The tmnxlomEventOverflowClr 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. |

12.209 tmnxlomResExhausted

Table 363: tmnxlomResExhausted properties

| Property name | Value |
|------------------|---------|
| Application name | CHASSIS |

| Property name | Value |
|----------------------------------|---|
| Event ID | 2122 |
| Event name | tmnxlomResExhausted |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.109 |
| Default severity | critical |
| Source stream | main |
| Message format string | The <i>\$tmnxlomResourceType\$</i> resources on IOM <i>\$tmnxChassisNotifyCardSlotNum\$</i> and Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> has been exhausted at <i>\$tmnxlomResLimitTimeEventOccured\$</i> . |
| Cause | The tmnxlomResExhausted notification is generated when the type of resources on IOM as specified by tmnxlomResourceType 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. |

12.210 tmnxlomResHighLimitReached

Table 364: *tmnxlomResHighLimitReached* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2121 |
| Event name | tmnxlomResHighLimitReached |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.108 |
| Default severity | major |
| Source stream | main |
| Message format string | The <i>\$tmnxlomResourceType\$</i> resources on IOM <i>\$tmnxChassisNotifyCardSlotNum\$</i> and Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> has reached the <i>\$tmnxlomResourceLimitPct\$%</i> utilization threshold at <i>\$tmnxlomResLimitTimeEventOccured\$</i> . |
| Cause | The tmnxlomResHighLimitReached notification is generated when the resource (of type tmnxlomResourceType) utilization on IOM has reached the value of tmnxlomResourceLimitPct. |

| 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. |

12.211 tmnxlomResStateClr

Table 365: *tmnxlomResStateClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2123 |
| Event name | tmnxlomResStateClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.110 |
| Default severity | minor |
| Source stream | main |
| Message format string | The <i>\$tmnxlomResourceType\$</i> resources on IOM <i>\$tmnxChassisNotifyCardSlotNum\$</i> and Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> has dropped below the <i>\$tmnxlomResourceLimitPct\$%</i> utilization threshold at <i>\$tmnxlomResLimitTimeEventOccured\$</i> . |
| Cause | The tmnxlomResStateClr notification is generated when the type of resources on IOM as specified by tmnxlomResourceType has dropped back down below the value of tmnxlomResourceLimitPct. |
| Effect | The specified resource limit is cleared when the number of in-use stats resources falls below tmnxlomResourceLimitPct of the stats pool limit. |
| Recovery | There is no recovery required for this notification. |

12.212 tmnxlomRsrcEventOverflow

Table 366: *tmnxlomRsrcEventOverflow* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 3257 |
| Event name | tmnxlomRsrcEventOverflow |
| 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 <i>\$tmnxChassisNotifyCard SlotNum\$</i> at <i>\$tmnxlomRsrcTimeEventOccured\$</i> . |
| Cause | The tmnxlomRsrcEventOverflow notification is generated when tmnx lomRsrcUsageHighLimitReached, tmnxlomRsrcUsageExhausted, tmnxlomRsrcUsageRecovered, tmnxlomRsrcOwnerOversubscribed, or tmnxlomRsrcOwnerOversubscrbdClr 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. |

12.213 tmnxlomRsrcEventOverflowClr

Table 367: *tmnxlomRsrcEventOverflowClr* properties

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

| Property name | Value |
|-----------------------|--|
| Message format string | <i>\$tmnxlomRsrcMissingNotifCount\$</i> resource events were dropped in the last event throttling interval on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxlomRsrcTimeEventOccured\$</i> . |
| Cause | The <i>tmnxlomRsrcEventOverflowClr</i> 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. |

12.214 tmnxlomRsrcOwnerOversubscrbdClr

Table 368: *tmnxlomRsrcOwnerOversubscrbdClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 3260 |
| Event name | <i>tmnxlomRsrcOwnerOversubscrbdClr</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.262</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | The <i>\$tmnxlomRsrcResourceType\$</i> resources needed by <i>\$tmnxlomRsrcOwnerType\$</i> on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> have been satisfied at <i>\$tmnxlomRsrcTimeEventOccured\$</i> . All <i>\$tmnxlomRsrcOwnerType\$</i> traffic can flow. |
| Cause | The <i>tmnxlomRsrcOwnerOversubscrbdClr</i> notification is generated when all the required IOM resources of type <i>tmnxlomRsrcResourceType</i> for owner <i>tmnxlomRsrcOwnerType</i> have been allocated. |
| Effect | Traffic for owner <i>tmnxlomRsrcOwnerType</i> is no longer affected. |
| Recovery | There is no recovery for this notification. |

12.215 tmnxlomRsrcOwnerOversubscribed

Table 369: *tmnxlomRsrcOwnerOversubscribed* properties

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

12.216 tmnxlomRsrcUsageExhausted

Table 370: *tmnxlomRsrcUsageExhausted* properties

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

| Property name | Value |
|-----------------------|--|
| Source stream | main |
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> The <i>\$tmnxlomRsrcResourceType\$</i> resources on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> have been exhausted at <i>\$tmnxlomRsrcTimeEventOccured\$</i>. The <i>\$tmnxlomRsrcResourceType\$</i> resources on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> have been exhausted at <i>\$tmnxlomRsrcTimeEventOccured\$</i>. Current utilization is <i>\$tmnxlomRsrcUsagePercent\$</i>%. |
| Cause | The <i>tmnxlomRsrcUsageExhausted</i> notification is generated when all the IOM resources of type <i>tmnxlomRsrcResourceType</i> 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. |

12.217 tmnxlomRsrcUsageHighLimitReached

Table 371: *tmnxlomRsrcUsageHighLimitReached* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 3252 |
| Event name | tmnxlomRsrcUsageHighLimitReached |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.252 |
| Default severity | warning |
| Source stream | main |
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> The <i>\$tmnxlomRsrcResourceType\$</i> resources on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> have reached or exceeded the high utilization threshold at <i>\$tmnxlomRsrcTimeEventOccured\$</i>. The <i>\$tmnxlomRsrcResourceType\$</i> resources on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> Forwarding Plane <i>\$tmnxChassisNotifyFpNum\$</i> have reached or exceeded the high utilization threshold at <i>\$tmnxlomRsrcTimeEventOccured\$</i>. |

| Property name | Value |
|---------------|--|
| | <i>FpNum</i> have reached or exceeded the high utilization threshold at <i>\$tmnxlomRsrcTimeEventOccured</i> . Current utilization is <i>\$tmnxlomRsrcUsagePercent</i> %. |
| Cause | The <i>tmnxlomRsrcUsageHighLimitReached</i> notification is generated when the utilization of the IOM resource of type <i>tmnxlomRsrcResourceType</i> 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. |

12.218 tmnxlomRsrcUsageRecovered

Table 372: *tmnxlomRsrcUsageRecovered* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 3254 |
| Event name | <i>tmnxlomRsrcUsageRecovered</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.254</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> The <i>\$tmnxlomRsrcResourceType</i> resources on card <i>\$tmnxChassisNotifyCardSlotNum</i> Forwarding Plane <i>\$tmnxChassisNotifyFpNum</i> have dropped below the warning utilization threshold at <i>\$tmnxlomRsrcTimeEventOccured</i>. The <i>\$tmnxlomRsrcResourceType</i> resources on card <i>\$tmnxChassisNotifyCardSlotNum</i> Forwarding Plane <i>\$tmnxChassisNotifyFpNum</i> have dropped below the warning utilization threshold at <i>\$tmnxlomRsrcTimeEventOccured</i>. Current utilization is <i>\$tmnxlomRsrcUsagePercent</i>%. |
| Cause | The <i>tmnxlomRsrcUsageRecovered</i> notification is generated when the utilization of the IOM resource of type <i>tmnxlomRsrcResourceType</i> 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. |

12.219 tmnxIPMacCpmFilterOverload

Table 373: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.220 tmnxIPMacCpmFilterOverloadClear

Table 374: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> no longer has an IPv4 or MAC CPM Filter in overload. |
| Cause | The <i>tmnxIPMacCpmFilterOverloadClear</i> 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. |

12.221 *tmnxIPMacFilterEgrNearFull*

Table 375: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.222 tmnxIPMacFilterEgrNearFullClear

Table 376: 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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.223 tmnxIPMacFilterEgrOverload

Table 377: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.224 tmnxIPMacFilterEgrOverloadClear

Table 378: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> no longer has an egress IPv4 or MAC ACL Filter in overload. |
| Cause | The <i>tmnxIPMacFilterEgrOverloadClear</i> 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. |

12.225 tmnxIPMacFilterIngNearFull

Table 379: *tmnxIPMacFilterIngNearFull* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2275 |
| Event name | <i>tmnxIPMacFilterIngNearFull</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.197</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Slot <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> has ingress IPv4 or MAC ACL Filters at near full utilization. |
| Cause | The <i>tmnxIPMacFilterIngNearFull</i> 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. |

12.226 tmnxIPMacFilterIngNearFullClear

Table 380: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> no longer has ingress IPv4 or MAC ACL Filters at near full utilization. |
| Cause | The <i>tmnxIPMacFilterIngNearFullClear</i> 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. |

12.227 *tmnxIPMacFilterIngOverload*

Table 381: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.228 tmnxIPMacFilterIngOverloadClear

Table 382: 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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.229 tmnxIPMacQosIngOverload

Table 383: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.230 tmnxIPMacQosIngOverloadClear

Table 384: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> no longer has an ingress QoS policy with IPv4 or MAC criteria entries in overload. |
| Cause | The <i>tmnxIPMacQosIngOverloadClear</i> 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. |

12.231 tmnxIPQosEgrOverload

Table 385: *tmnxIPQosEgrOverload* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2169 |
| Event name | <i>tmnxIPQosEgrOverload</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.158</i> |
| Default severity | major |
| Source stream | main |
| Message format string | Slot <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> has an egress QoS policy with IPv4 criteria entries in overload. |
| Cause | The <i>tmnxIPQosEgrOverload</i> 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. |

12.232 tmnxIPQosEgrOverloadClear

Table 386: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> \$ 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. |

12.233 tmnxIPseclsaGrpActivelsaChgd

Table 387: *tmnxIPseclsaGrpActivelsaChgd* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2062 |
| Event name | tmnxIPseclsaGrpActivelsaChgd |
| 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 <i>\$tmnxIPseclsaGrpActiveIsa\$</i> for IPsec ISA group <i>\$tmnxIPseclsaGrpId\$</i> where primary ISA is <i>\$tmnxIPseclsaGrpPrimaryIsa\$</i> and Backup ISA is <i>\$tmnxIPseclsaGrpBackupIsa\$</i> |
| Cause | The <i>tmnxIPseclsaGrpActiveIsaChgd</i> 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 |

12.234 tmnxIPseclsaGrpTnlHighWMark

Table 388: *tmnxIPseclsaGrpTnlHighWMark* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 2066 |
| Event name | tmnxIPseclsaGrpTnlHighWMark |
| 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 <i>\$tmnxIPsecIsaGrpId\$</i> has reached to the high watermark which is 95% of the maximum limit <i>\$tmnxIPseclsaGrpMaxTunnels\$</i> . |
| 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 |

12.235 tmnxIPsecIsaGrpTnlLowWMark

Table 389: *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 <i>\$tmnxIPsecIsaGrpId\$</i> has dropped to the low watermark which is 90% of the maximum limit <i>\$tmnxIPsecIsaGrpMaxTunnels\$</i> . |
| 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 |

12.236 tmnxIPsecIsaGrpTnlMax

Table 390: *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 <i>\$tmnxIPsecIsaGrpId\$</i> has reached the maximum limit <i>\$tmnxIPsecIsaGrpMaxTunnels\$</i> . |
| Cause | The number of tunnels for an IPsec ISA (Integrated Service Adaptor) module has reached the maximum limit. |
| Effect | N/A |
| Recovery | N/A |

12.237 tmnxIPseclsaGrpUnableToSwitch

Table 391: *tmnxIPseclsaGrpUnableToSwitch* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2064 |
| Event name | tmnxIPseclsaGrpUnableToSwitch |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.52 |
| Default severity | minor |
| Source stream | main |
| Message format string | IPsec ISA <i>\$tmnxIPseclsaGrpActiveIsa\$</i> for group <i>\$tmnxIPseclsaGrpId\$</i> 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 <i>tmnxIPseclsaGrpOperState</i> is set to 'outOfService'. |
| Recovery | Recovery is possible by releasing resources and performing a shutdown/no shutdown operation to bring up the ISA group. |

12.238 tmnxIPv6CpmFilterOverload

Table 392: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> has an IPv6 CPM Filter in overload. |
| Cause | The <i>tmnxIPv6CpmFilterOverload</i> 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. |

12.239 *tmnxIPv6CpmFilterOverloadClear*

Table 393: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> no longer has an IPv6 CPM Filter in overload. |
| Cause | The <i>tmnxIPv6CpmFilterOverloadClear</i> 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. |

12.240 tmnxIPv6FilterEgrNearFull

Table 394: *tmnxIPv6FilterEgrNearFull* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2281 |
| Event name | <i>tmnxIPv6FilterEgrNearFull</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.203</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Slot <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> has egress IPv6 ACL Filters at near full utilization. |
| Cause | The <i>tmnxIPv6FilterEgrNearFull</i> 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. |

12.241 tmnxIPv6FilterEgrNearFullClear

Table 395: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> no longer has egress IPv6 ACL Filters at near full utilization. |
| Cause | The <i>tmnxIPv6FilterEgrNearFullClear</i> 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. |

12.242 *tmnxIPv6FilterEgrOverload*

Table 396: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.243 tmnxIPv6FilterEgrOverloadClear

Table 397: 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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.244 tmnxIPv6FilterIngNearFull

Table 398: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> has ingress IPv6 ACL Filters at near full utilization. |
| Cause | The <i>tmnxIPv6FilterIngNearFull</i> 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. |

12.245 *tmnxIPv6FilterIngNearFullClear*

Table 399: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.246 tmnxIPv6FilterIngOverload

Table 400: 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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.247 tmnxIPv6FilterIngOverloadClear

Table 401: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.248 tmnxIPv6QosEgrOverload

Table 402: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.249 tmnxIPv6QoSEgrOverloadClear

Table 403: 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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.250 tmnxIPv6QosIngOverload

Table 404: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.251 tmnxIPv6QosIngOverloadClear

Table 405: *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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> FP <i>\$tmnxChassisNotifyFpNum\$</i> 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. |

12.252 tmnxIxrResourceExhausted

Table 406: *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 <i>\$tmnxNotifIxrResource\$</i> 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. |

12.253 tmnxlrxResourceExhaustedByOwner

Table 407: *tmnxlrxResourceExhaustedByOwner* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2436 |
| Event name | tmnxlrxResourceExhaustedByOwner |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.301 |
| Default severity | critical |
| Source stream | main |
| Message format string | The <i>\$tmnxNotiflrxResource\$</i> resources needed by <i>\$tmnxNotiflrxResourceOwner\$</i> have been exhausted. Some <i>\$tmnxNotiflrxResourceOwner\$</i> traffic may be affected. |
| Cause | The tmnxlrxResourceExhaustedByOwner notification is generated when the utilization of the resource specified by tmnxNotiflrxResource reached its limit for application specified by tmnxNotiflrxResourceOwner. |
| Effect | Usage of the resource specified by tmnxNotiflrxResource reached its limit for application specified by tmnxNotiflrxResourceOwner. |
| Recovery | Intervention may be required to recover resources. |

12.254 tmnxlrxResourceHighUsage

Table 408: *tmnxlrxResourceHighUsage* properties

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

| Property name | Value |
|-----------------------|---|
| Default severity | major |
| Source stream | main |
| Message format string | The <i>\$tmnxNotiflXrResource\$</i> resources have reached or exceeded the high utilization threshold. Current utilization is <i>\$tmnxNotiflXrRsrcUtilPercentage\$%%</i> . |
| Cause | The <i>tmnxlXrResourceHighUsage</i> 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. |

12.255 tmnxlXrResourceHighUsageByOwner

Table 409: *tmnxlXrResourceHighUsageByOwner* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2435 |
| Event name | <i>tmnxlXrResourceHighUsageByOwner</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.300</i> |
| Default severity | major |
| Source stream | main |
| Message format string | The <i>\$tmnxNotiflXrResource\$</i> resources needed by <i>\$tmnxNotiflXrResourceOwner\$</i> have reached or exceeded the high utilization threshold. Current utilization is <i>\$tmnxNotiflXrRsrcUtilPercentage\$%%</i> . |
| Cause | The <i>tmnxlXrResourceHighUsageByOwner</i> 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. |

12.256 tmnxIxrResourceRecovered

Table 410: *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 <i>\$tmnxNotifIxrResource\$</i> resources have dropped below the warning utilization threshold. Current utilization is <i>\$tmnxNotifIxrRsrcUtil Percentage\$%%</i> . |
| 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. |

12.257 tmnxIxrResourceRecoveredByOwner

Table 411: *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 <i>\$tmnxNotiflXrResource\$</i> resources needed by <i>\$tmnxNotiflXrResourceOwner\$</i> have dropped below the warning utilization threshold. Current utilization is <i>\$tmnxNotiflXrResourceOwner\$</i> %. |
| Cause | The <i>tmnxlXrResourceRecoveredByOwner</i> 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 <i>tmnxlXrResourceHighUsageByOwner</i> notification or the <i>tmnxlXrResourceExhaustedByOwner</i> 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. |

12.258 tmnxMDAIsaTunnelGroupChange

Table 412: *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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxMDASlotNum\$</i> is <i>\$tmnxMDAIsaTunnelGroupInUse\$</i> active in the ISA tunnel-group <i>\$tmnxMDAIsaTunnelGroup\$</i> |
| Cause | The <i>tmnxMDAIsaTunnelGroupChange</i> 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 |

12.259 tmnxPeBootloaderVersionMismatch

Table 413: *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 <i>\$tmnxHwClass\$</i> : Bootloader version mismatch - expected software version <i>\$tmnxHwSoftwareCodeVersion\$</i> , equipped version <i>\$tmnxChassisNotifyMismatchedVer\$</i> |
| Cause | Generated when there is a mismatch between the CPM and boot loader versions. <i>tmnxChassisNotifyHwIndex</i> identifies the CPM card. <i>tmnxChassisNotifyMismatchedVer</i> contains the mismatched version of bootloader and <i>tmnxHwSoftwareCodeVersion</i> contains the expected version of the bootloader. |
| Effect | N/A |
| Recovery | N/A |

12.260 tmnxPeBootromVersionMismatch

Table 414: *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 <i>\$tmnxHwClass\$</i> : Bootrom version mismatch - expected version <i>\$tmnxHwSoftwareCodeVersion\$</i> , equipped version <i>\$tmnxChassisNotifyMismatchedVer\$</i> |
| Cause | Generated when there is a mismatch between the boot rom versions. <i>tmnxChassisNotifyHwIndex</i> identifies the IOM card. <i>tmnxChassisNotifyMismatchedVer</i> contains the mismatched version of bootrom and <i>tmnxHwSoftwareCodeVersion</i> contains the expected version of the bootrom. |
| Effect | N/A |
| Recovery | N/A |

12.261 tmnxPeFirmwareVersionWarning

Table 415: *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 <i>\$tmnxHwClass\$</i> : Firmware version <i>\$tmnxHwFirmwareCodeVersion\$</i> 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. <i>tmnxChassisNotifyHwIndex</i> identifies the card. The <i>tmnxHwFirmwareCodeVersion</i> object will contain the programmed the firmware version. |
| Effect | N/A |
| Recovery | N/A |

12.262 tmnxPeFPGAVersionMismatch

Table 416: *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 <i>\$tmnxHwClass\$</i> : FPGA version mismatch - expected version <i>\$tmnxHwSoftwareCodeVersion\$</i> , equipped version <i>\$tmnxChassisNotifyMismatchedVer\$</i> |
| Cause | Generated when there is a mismatch between the FPGA versions. <i>tmnxChassisNotifyHwIndex</i> identifies the IOM card. <i>tmnxChassisNotifyMismatchedVer</i> contains the mismatched version of FPGA and <i>tmnxHwSoftwareCodeVersion</i> contains the expected version of the FPGA. |
| Effect | N/A |
| Recovery | N/A |

12.263 tmnxPeKernelVersionMismatch

Table 417: *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 <i>\$tmnxHwClass\$</i> : Kernel version mismatch - expected software version <i>\$tmnxHwSoftwareCodeVersion\$</i> , equipped version <i>\$tmnxChassisNotifyMismatchedVer\$</i> |
| 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 <i>tmnxChassisNotifyHwIndex</i> identifies the CPM card. The object <i>tmnxChassisNotifyMismatchedVer</i> contains the version of the host kernel software and <i>tmnxHwSoftwareCodeVersion</i> 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. |

12.264 tmnxPeSoftwareLoadFailed

Table 418: *tmnxPeSoftwareLoadFailed* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2026 |
| Event name | <i>tmnxPeSoftwareLoadFailed</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification</i> .34 |
| Default severity | major |
| Source stream | main |
| Message format string | Class <i>\$tmnxHwClass\$</i> : Failed to load software from <i>\$tmnxChassisNotifySoftwareLocation\$</i> |

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

12.265 `tmnxPeSoftwareVersionMismatch`

Table 419: `tmnxPeSoftwareVersionMismatch` properties

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

12.266 `tmnxPhysChassisFilterDoorClosed`

Table 420: *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. |

12.267 tmnxPhysChassisFilterDoorOpen

Table 421: *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. |

12.268 tmnxPhysChassisPCMInputFeed

Table 422: *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 <i>\$tmnxPhysChassisNum\$</i> pcm <i>\$tmnxPhysChassisPCMIId\$</i> <i>\$tmnxPhysChassisPCMInFeedDown\$</i> 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. |

12.269 tmnxPhysChassisPCMInputFeedClr

Table 423: *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 <i>\$tmnxPhysChassisNum\$</i> pcm <i>\$tmnxPhysChassisPCMIId\$</i> are supplying power. |
| Cause | The <i>tmnxPhysChassisPCMInputFeedClr</i> 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. |

12.270 tmnxPhysChassisPMInputFeed

Table 424: *tmnxPhysChassisPMInputFeed* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2192 |
| Event name | <i>tmnxPhysChassisPMInputFeed</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.191</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Power module <i>\$tmnxHwIndex\$</i> <i>\$tmnxPhysChassisPMInputFeedDown</i> \$not supplying power. |
| Cause | The <i>tmnxPhysChassisPMInputFeed</i> 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. |

12.271 tmnxPhysChassisPMInputFeedClr

Table 425: *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 <i>\$tmnxHwIndex\$</i> 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. |

12.272 tmnxPhysChassisPMOutFail

Table 426: *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 <i>\$tmnxHwIndex\$</i> 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. |

12.273 tmnxPhysChassisPMOutFailClr

Table 427: *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 <i>\$tmnxHwIndex\$</i> 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. |

12.274 tmnxPhysChassisPMOverTemp

Table 428: *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 | <i>\$tmnxHwIndex\$</i> 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. |

12.275 tmnxPhysChassisPMOverTempClr

Table 429: *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 | <i>\$tmnxHwIndex\$</i> 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. |

12.276 tmnxPhysChassPwrSupInputFeed

Table 430: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupld\$</i> <i>\$tmnxPhysChassPowerSuplnFeedDown\$</i> 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. |

12.277 tmnxPhysChassPwrSupInputFeedClr

Table 431: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupld\$</i> 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. |

12.278 tmnxPhysChassPwrSupPemACRect

Table 432: 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 \$tmnxPhysChassPowerSupld\$ \$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. |

12.279 tmnxPhysChassPwrSupPemACRectClr

Table 433: *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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupId\$</i> 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. |

12.280 tmnxPhysChassPwrSupWrgFanDir

Table 434: *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 <i>\$tmnxPhysChassPowerSupFanDir\$</i> fan direction for chassis <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupId\$</i> 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. |

12.281 tmnxPhysChassPwrSupWrgFanDirClr

Table 435: 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 <i>\$tmnxPhysChassisNum\$</i> power supply <i>\$tmnxPhysChassPowerSupId\$</i> 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. |

12.282 tmnxPlcyAcctPlcrPoolExcResource

Table 436: 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 <i>\$tmnxCardSlotNum\$</i> and forwarding plane <i>\$tmnxFPNum\$</i> exceeds 95 percent of the policer limit. Total policer resource used is ' <i>\$tmnxFPPlcyAcctPolicerInUse\$</i> ' and the limit is ' <i>\$tmnxFPPlcyAcctPolicerLimit\$</i> ' |
| 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. |

12.283 tmnxPlcyAcctPlcrPoolLowResource

Table 437: 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 <i>\$tmnxCardSlotNum\$</i> and forwarding plane <i>\$tmnxFPNum\$</i> is below 85 percent of the policer limit. Total policer resource used is ' <i>\$tmnxFPPlcyAcctPolicerInUse\$</i> ' and the limit is ' <i>\$tmnxFPPlcyAcctPolicerLimit\$</i> ' |

| Property name | Value |
|---------------|--|
| Cause | The tmnxPlcyAcctPlcrPoolLowResource notification is generated when the number of in-use policer resource as specified by tmnxFPPlcyAcctPolicerInUse 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. |

12.284 tmnxPlcyAcctStatsEventOvrflw

Table 438: 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 \$tmnxChassisNotifyCardSlotNum\$ at \$tmnxPlcyAcctTimeEventOccured\$. |
| Cause | The tmnxPlcyAcctStatsEventOvrflw notification is generated when tmnxPlcyAcctStatsPoolExcResource and tmnxPlcyAcctStatsPoolLowResource 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. |

12.285 tmnxPlcyAcctStatsEventOvrflwClr

Table 439: *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 | <i>\$tmnxPlcyAcctMissingNotifCount\$</i> Policy Accounting FP log events were dropped in the last event throttling interval on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxPlcyAcctTimeEventOccured\$</i> . |
| 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. |

12.286 tmnxPlcyAcctStatsPoolExcResource

Table 440: *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 <i>\$tmnxCardSlotNum\$</i> and forwarding plane <i>\$tmnxFPNum\$</i> 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. |

12.287 tmnxPlcyAcctStatsPoolLowResource

Table 441: 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 tmnxFPPlcyAcctStatsInUse 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. |

12.288 tmnxPowerShelfCommsDown

Table 442: *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 | <i>\$tmnxHwIndex\$</i> lost communication with <i>\$tmnxCpmPowerShelfCommsFail\$</i> |
| 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. |

12.289 tmnxPowerShelfCommsUp

Table 443: *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 <i>\$tmnxHwIndex\$</i> |
| 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. |

12.290 tmnxPowerShelfInputPwrModeSwitch

Table 444: *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 | <i>\$tmnxHwIndex\$</i> input power mode switched to <i>\$tmnxPowerShelfInputPowerMode\$A</i> |
| Cause | The tmnxPowerShelfInputPwrModeSwitch is generated when tmnxPowerShelfInputPowerMode has changed value. |
| Effect | No effect. |
| Recovery | No recovery required. |

12.291 tmnxPowerShelfOutputStatusDown

Table 445: *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 | <i>\$tmnxHwIndex\$</i> output status switched to <i>\$tmnxPowerShelfOutput Status\$</i> |
| 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. |

12.292 tmnxPowerShelfOutputStatusSwitch

Table 446: *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 | <i>\$tmnxHwIndex\$</i> output status switched to <i>\$tmnxPowerShelfOutput Status\$</i> |

| Property name | Value |
|---------------|--|
| Cause | The tmnxPowerShelfOutputStatusSwitch is generated when tmnxPowerShelfOutputStatus has changed value. |
| Effect | No effect. |
| Recovery | No recovery required. |

12.293 tmnxPowerShelfOutputStatusUp

Table 447: 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 | <i>\$tmnxHwIndex\$</i> output status switched to <i>\$tmnxPowerShelfOutputStatus\$</i> |
| 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. |

12.294 tmnxPowerSupplyFanFailed

Table 448: 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 <i>\$tmnxHwIndex\$</i> 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. |

12.295 tmnxPowerSupplyFanFailedClear

Table 449: *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 <i>\$tmnxHwIndex\$</i> 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 |

12.296 tmnxRedPrimaryCPMFail

Table 450: *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 |

12.297 tmnxSasAlarminput1StateChanged

Table 451: *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. |

12.298 tmnxSasAlarmInput2StateChanged

Table 452: 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. |

12.299 tmnxSasAlarminput3StateChanged

Table 453: *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. |

12.300 tmnxSasAlarminput4StateChanged

Table 454: 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. |

12.301 tmnxSfmlcPortDDMClear

Table 455: tmnxSfmlcPortDDMClear properties

| Property name | Value |
|------------------|---------|
| Application name | CHASSIS |

| Property name | Value |
|----------------------------------|--|
| Event ID | 4026 |
| Event name | tmnxSfmlcPortDDMClear |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.7 |
| Default severity | minor |
| Source stream | main |
| Message format string | SFM interconnect port SFF DDM <i>\$tmnxDDMLaneIdOrModule\$ (\$tmnxDDMFailedObject\$)</i> cleared |
| Cause | The tmnxSfmlcPortDDMFailure 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 |

12.302 tmnxSfmlcPortDDMFailure

Table 456: *tmnxSfmlcPortDDMFailure* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4025 |
| Event name | tmnxSfmlcPortDDMFailure |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.6 |
| Default severity | minor |
| Source stream | main |
| Message format string | SFM interconnect port SFF DDM <i>\$tmnxDDMLaneIdOrModule\$ (\$tmnxDDMFailedObject\$)</i> raised |
| Cause | The tmnxSfmlcPortDDMFailure 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 |

12.303 tmnxSfmlcPortDegraded

Table 457: *tmnxSfmlcPortDegraded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4027 |
| Event name | tmnxSfmlcPortDegraded |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.8 |
| Default severity | minor |
| Source stream | main |
| Message format string | Switch fabric capacity associated with the SFM interconnect port is in a <i>\$tmnxSfmlcPortDegradedState\$</i> state |
| Cause | The tmnxSfmlcPortDegraded 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 tmnxSfmlcPortDegradedState will reflect this condition by having a value that is NOT 'none (1)'. If the value of tmnxSfmlcPortDegradedState 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 tmnxSfmlcPortDegradedState 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." |

12.304 tmnxSfmlcPortDegradedClear

Table 458: *tmnxSfmlcPortDegradedClear* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4028 |
| Event name | tmnxSfmlcPortDegradedClear |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort 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 tmnxSfmlcPortDegradedClear notification is generated when the switch fabric associated with the SFM interconnect port is not degraded. This occurs when the value of tmnxSfmlcPortDegradeState is 'none (1)'." |
| Effect | N/A |
| Recovery | N/A |

12.305 tmnxSfmlcPortDown

Table 459: *tmnxSfmlcPortDown* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4017 |
| Event name | tmnxSfmlcPortDown |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.1 |
| Default severity | minor |
| Source stream | main |
| Message format string | Possible messages: |

| Property name | Value |
|---------------|--|
| | <ul style="list-style-type: none"> SFM interconnect port is not operational. Error code = <i>\$tmnxSfmIcPortOperState\$</i> to Fabric <i>\$tmnxSfmIcPortMisconSfm\$IcPort\$tmnxSfmIcPortMisconSfmIcPort\$</i> SFM interconnect port is not operational. Error code = <i>\$tmnxSfmIcPortOperState\$</i> |
| Cause | The <i>tmnxSfmIcPortDown</i> 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. |

12.306 *tmnxSfmIcPortSFFInserted*

Table 460: *tmnxSfmIcPortSFFInserted* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4019 |
| Event name | <i>tmnxSfmIcPortSFFInserted</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB. <i>tmnxSfmIcPortNotifications.3</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | SFM interconnect port SFF inserted |
| Cause | The <i>tmnxSfmIcPortSFFInserted</i> 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 |

12.307 tmnxSfmlcPortSFFRemoved

Table 461: *tmnxSfmlcPortSFFRemoved* properties

| Property name | Value |
|----------------------------------|---|
| Application name | CHASSIS |
| Event ID | 4020 |
| Event name | tmnxSfmlcPortSFFRemoved |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.4 |
| Default severity | minor |
| Source stream | main |
| Message format string | SFM interconnect port SFF removed |
| Cause | The tmnxSfmlcPortSFFRemoved 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. |

12.308 tmnxSfmlcPortUp

Table 462: *tmnxSfmlcPortUp* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 4018 |
| Event name | tmnxSfmlcPortUp |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-INTERCONNECT-MIB.tmnxSfmlcPort Notifications.2 |
| Default severity | minor |

| Property name | Value |
|-----------------------|--|
| Source stream | main |
| Message format string | SFM interconnect port is operational |
| Cause | The tmnxSfmlcPortUp 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 |

12.309 tmnxSynclfTimBITS2048khzUnsup

Table 463: tmnxSynclfTimBITS2048khzUnsup properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2134 |
| Event name | tmnxSynclfTimBITS2048khzUnsup |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.123 |
| Default severity | major |
| Source stream | main |
| Message format string | The revision of <i>\$tmnxHwIndex\$</i> does not meet the specifications to support the 2048kHz BITS interface type. |
| Cause | The tmnxSynclfTimBITS2048khzUnsup notification is generated when the value of tSynclfTimingAdmBITSIfType 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 tSynclfTimingAdmBITSIfType to a value other than 'g703-2048khz (5)'. |

12.310 tmnxSynclfTimBITS2048khzUnsupClr

Table 464: *tmnxSynclfTimBITS2048khzUnsupClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | CHASSIS |
| Event ID | 2135 |
| Event name | tmnxSynclfTimBITS2048khzUnsupClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.124 |
| Default severity | major |
| Source stream | main |
| Message format string | <i>\$tmnxHwIndex\$</i> has been replaced with a CPM that meets the specification for 2048kHz or the BITS interface type is no longer 2048k Hz. |
| Cause | The tmnxSynclfTimBITS2048khzUnsupClr notification is generated when a tmnxSynclfTimBITS2048khzUnsup notification is outstanding and the CPM was replaced with one that meets the specifications for the 2048kHz BITS output signal under G.703 or tSynclfTiming AdmBITSIfType is set to a value other than 'g703-2048khz (5)'. |
| Effect | The CPM can now support the configuration of tSynclfTiming AdmBITSIfType. |
| Recovery | No recovery required. |

12.311 tmnxTunnelGrpEsaVmActivity

Table 465: *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- <i>\$tmnxEsald\$</i> / <i>\$tmnxEsaVmId\$</i> is <i>\$tmnxTunnelGrpEsaVmActive\$</i> in tunnel group <i>\$tmnxTunnelGrpEsaVmGroupAssoc\$</i> |
| Cause | The <i>tmnxTunnelGrpEsaVmActivity</i> 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 466: 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 | <i>\$subject\$: \$title\$ \$message\$</i> |
| Cause | The system generated a debug message. |
| Effect | Unknown. |
| Recovery | Contact Nokia customer service. |

14 DHCP

14.1 sapDHCPLeaseEntriesExceeded

Table 467: 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 \$svclId\$ 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 sapDHCPLeaseStateMobilityError

Table 468: 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> |
| 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 469: 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 = <i>\$svcDhcpLseStateOldCiAddr\$</i> , macAddr = <i>\$svcDhcpLseStateOldChAddr\$</i>) on SAP <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> overridden to (ipAddr = <i>\$svcDhcpLseStateNewCiAddr\$</i> , mac Addr = <i>\$svcDhcpLseStateNewChAddr\$</i>) |

| Property name | Value |
|---------------|---|
| Cause | The sapDHCPLeaseStateOverride 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 sapDHCPLeaseStatePopulateErr

Table 470: sapDHCPLeaseStatePopulateErr properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| Event ID | 2005 |
| Event name | sapDHCPLeaseStatePopulateErr |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$ - \$svcDhcpLeaseStatePopulateError\$</i> |
| Cause | The sapDHCPLeaseStatePopulateErr 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 471: 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> - <i>\$svcDhcpProxyError\$</i> |
| 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 472: 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> - <i>\$svcDhcpPacketProblem\$</i> |
| 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 473: 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 <i>\$sapStatHost6IpAddress\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svcId\$</i> - <i>\$sapNotifyReason\$</i> |
| 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 474: 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 <i>\$staticHostDynamicMacIpAddress\$</i> on SAP <i>\$sapEncapValue\$</i> (service <i>\$svcId\$</i>) - <i>\$staticHostDynamicMacConflict\$</i> |
| 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 475: 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 = <i>\$svcDhcpLseStateNewCiAddr\$</i> , ChAddr = <i>\$svcDhcpLseStateNewChAddr\$</i> , leaseTime = <i>\$svcDhcpClientLease\$</i>) was not stored because the number of DHCP lease states on SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> 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 476: 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> |
| 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 477: 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 sdpBindDHCPLeaseStateOverride 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 sdpBindDHCPLeaseStatePopulateErr

Table 478: sdpBindDHCPLeaseStatePopulateErr properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2009 |
| Event name | sdpBindDHCPLeaseStatePopulateErr |
| 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 sdpBindDHCPLeaseStatePopulateErr 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 479: 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> - <i>\$svcDhcpProxyError\$</i> |
| 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 480: 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> - <i>\$svcDhcpPacketProblem\$</i> |
| 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 481: *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 = <i>\$svcDhcpRestoreLseStateCiAddr\$</i>) - <i>\$svcDhcpRestoreLseStateProblem\$</i> |
| 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 482: *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 | <i>\$tmnxFailureDescription\$</i> |
| Cause | The svcDHCPMiscellaneousProblem notification is generated on miscellaneous DHCP problems. |
| Effect | N/A |
| Recovery | Contact Nokia customer service. |

14.17 tmnxVRtrDHCP6AssignedIllegSubnet

Table 483: *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 = <i>\$vRtrDHCP6AssignedNetAddr\$/\$vRtrDHCP6AssignedPrefixLen\$</i>) assigned to client (inetAddr = <i>\$vRtrDHCP6ClientNetAddr\$</i>) does not match the subnet of the incoming interface <i>\$vRtrIfName\$</i> , or conflicts with an existing node IP address in service <i>\$vRtrServiceId\$</i> (vRtr <i>\$vRtrID\$</i>) |

| 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 484: 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 485: *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 486: *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 |
|---------------|--|
| | <i>RtrIfName\$</i> in service <i>\$vRtrServiceId\$</i> (vRtr <i>\$vRtrID\$</i>) to (inetAddr = <i>\$vRtrDHCP6AssignedNetAddr\$</i> / <i>\$vRtrDHCP6AssignedPrefixLen\$</i> , chAddr = <i>\$vRtrDhcpLseStateNewChAddr\$</i> , DUID = <i>\$vRtrDHCP6NewClientId\$</i>) - <i>\$vRtrDHCP6LeaseOverrideResult\$</i> |
| Cause | The <i>tmnxVRtrDHCP6LseStateOverride</i> 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 487: *tmnxVRtrDHCP6RelayLseStExceeded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2020 |
| Event name | <i>tmnxVRtrDHCP6RelayLseStExceeded</i> |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB. <i>tmnxVRtrNotifications.21</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Lease state for (inetAddr = <i>\$vRtrDHCP6AssignedNetAddr\$</i> / <i>\$vRtrDHCP6AssignedPrefixLen\$</i> , DUID = <i>\$vRtrDHCP6NewClientId\$</i> , leaseTime = <i>\$svcDhcpClientLease\$</i>) was not stored because the number of DHCP6 relay lease states on interface <i>\$vRtrIfName\$</i> in service <i>\$vRtrServiceId\$</i> (vRtr <i>\$vRtrID\$</i>) has reached its upper limit of <i>\$vRtrIfDHCP6LeasePopulate\$</i> |
| Cause | The <i>tmnxVRtrDHCP6RelayLseStExceeded</i> notification is generated when the number of lease states populated by DHCP6 relay on an interface exceeds <i>vRtrIfDHCP6LeasePopulate</i> . |
| Effect | N/A |
| Recovery | Investigate the cause of the excessive DHCP lease states. |

14.22 tmnxVRtrDHCP6RelayReplyStripUni

Table 488: *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 489: *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 490: 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 491: 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 <i>\$vRtrIfIndex\$</i> in service <i>\$vRtrServiceId\$</i> - <i>\$vRtrDhcpPacketProblem\$</i> |
| Cause | The tmnxVRtrDHCPSuspiciousPcktRcvd notification is generated when a DHCP packet is received with suspicious content. |
| Effect | N/A |
| Recovery | Contact Nokia customer service. |

15 DHCP

15.1 tmnxDhcpAddrAllocationFailure

Table 492: tmnxDhcpAddrAllocationFailure properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2035 |
| Event name | tmnxDhcpAddrAllocationFailure |
| 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="\$tmnxDhcpSvrNotifPrimaryPool\$" sec-pool="\$tmnxDhcpSvrNotifSecondaryPool\$"). Reason: \$tmnxDhcpSvrNotifString\$ |
| Cause | The tmnxDhcpAddrAllocationFailure 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 tmnxDhcpFoLeaseUpdateFailed

Table 493: *tmnxDhcpFoLeaseUpdateFailed* properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| Event ID | 2008 |
| Event name | tmnxDhcpFoLeaseUpdateFailed |
| 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= <i>\$tmnxDhcpSvrNotifServerName\$</i> , ipAddr= <i>\$tmnxDhcpSvrNotifLeaseClientAddr\$</i>) sender (mac= <i>\$tmnxDhcpSvrNotifMsgHwAddress \$ DUID=0x \$tmnxDhcpSvrNotifClientDUID\$</i>) -- reason: <i>\$tmnxDhcpFoLeaseFailureReason\$</i> |
| Cause | The tmnxDhcpFoLeaseUpdateFailed 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; subnetNotFound : configure a valid subnet for this lease; rangeNotFound : configure a valid include range for this lease. |

15.3 tmnxDhcpFoStateChange

Table 494: *tmnxDhcpFoStateChange* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2007 |
| Event name | tmnxDhcpFoStateChange |
| SNMP notification prefix and OID | TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.7 |
| Default severity | warning |
| Source stream | main |
| Message format string | DHCP server <i>\$tmnxDhcpServerCfgServerName\$</i> changed failover state: <i>\$tmnxDhcpFoState\$</i> . |
| 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 tmnxDhcpLeaseOfferedExpired

Table 495: *tmnxDhcpLeaseOfferedExpired* properties

| Property name | Value |
|------------------|-------|
| Application name | DHCP |
| 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 496: tmnxDhcpsPacketDropped properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 tmnxDhcpPoolFoLeaseUpdateFailed

Table 497: tmnxDhcpPoolFoLeaseUpdateFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2025 |
| Event name | tmnxDhcpPoolFoLeaseUpdateFailed |
| 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=\$tmnxDhcpServerPoolName\$\$, ipAddr=\$tmnxDhcpSvrNotifLeaseClientAddr\$) sender (mac= \$tmnxDhcpSvrNotifMsgHwAddress\$ DUID=0x\$tmnxDhcpSvrNotifClientDUID\$) -- reason: \$tmnxDhcpFoLeaseFailureReason\$ |
| Cause | The tmnxDhcpPoolFoLeaseUpdateFailed 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 tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'. |
| Effect | N/A |
| Recovery | N/A |

15.7 tmnxDhcpPoolFoStateChange

Table 498: *tmnxDhcpPoolFoStateChange* properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| Event ID | 2024 |
| Event name | tmnxDhcpPoolFoStateChange |
| SNMP notification prefix and OID | TIMETRA-DHCP-SERVER-MIB.tmnxDhcpServerNotifications.24 |
| Default severity | warning |
| Source stream | main |
| Message format string | DHCP server <i>\$tmnxDhcpServerCfgServerName\$</i> pool <i>\$tmnxDhcpServerPoolName\$</i> changed failover state: <i>\$tmnxDhcpPoolFoState\$</i> . |
| Cause | The <i>tmnxDhcpPoolFoStateChange</i> 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 <i>tmnxDhcpServerCfgAddrType</i> set to 'ipv4(1)' or 'ipv6(2)'. |
| Effect | N/A |
| Recovery | N/A |

15.8 tmnxDhcpSvrDeclineStaticAddr

Table 499: *tmnxDhcpSvrDeclineStaticAddr* properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| 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= <i>\$tmnxDhcpSvrNotifServerName\$</i> , ipAddr= <i>\$tmnxDhcpSvrNotifLeaseClientAddr\$</i>) is declined by client (HwAddr= <i>\$tmnxDhcpSvrNotifMsgHwAddress\$</i>) |

| Property name | Value |
|---------------|---|
| Cause | The <code>tmnxDhcpSvrDeclineStaticAddr</code> 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 500: `tmnxDhcpSvrHostConflict` properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2002 |
| Event name | <code>tmnxDhcpSvrHostConflict</code> |
| SNMP notification prefix and OID | TIMETRA-DHCP-SERVER-MIB. <code>tmnxDhcpServerNotifications.2</code> |
| Default severity | warning |
| Source stream | main |
| Message format string | DHCP server <code>\$tmnxDhcpSvrNotifServerName\$</code> detects IP address assignment conflict for host (name= <code>\$tmnxDhcpSvrNotifHostName\$</code> , type= <code>\$tmnxDhcpSvrNotifHostType\$</code>) sender (mac= <code>\$tmnxDhcpSvrNotifMsgHwAddress\$</code>); ipAddr= <code>\$tmnxDhcpSvrNotifLeaseClientAddr\$</code> . <code>\$tmnxDhcpSvrNotifDescription\$</code> |
| Cause | The <code>tmnxDhcpSvrHostConflict</code> 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 <code>tmnxDhcpSvrHostConflict</code> notification is generated. This notification is only generated for DHCP server instances with the value of <code>tmnxDhcpServerCfgAddrType</code> set to 'ipv4(1)'. |
| Effect | N/A |
| Recovery | Investigate the cause of the address conflict. |

15.10 tmnxDhcpSvrIntLseConflict

Table 501: tmnxDhcpSvrIntLseConflict properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| 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 502: tmnxDhcpSvrLeaseCreate properties

| Property name | Value |
|------------------|------------------------|
| Application name | DHCP |
| 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="\$tmnxDhcpSvrNotifMsgHwAddress\$ DUID=0x\$tmnxDhcpSvrNotifClientDUID\$) configuration created |
| Cause | The tmnxDhcpSvrLeaseCreate notification is generated when a DHCP host is created. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'. |
| Effect | N/A |
| Recovery | N/A |

15.12 tmnxDhcpSvrLeaseDefaultTimers

Table 503: tmnxDhcpSvrLeaseDefaultTimers properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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= \$tmnxDhcpSvrNotifServerName\$, ipAddr=\$tmnxDhcpSvrNotifLeaseClientAddr\$) 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 <code>tmnxDhcpServerCfgAddrType</code> set to 'ipv4(1)' or 'ipv6(2)'. |
| Effect | N/A |
| Recovery | N/A |

15.13 tmnxDhcpSvrLeaseDelete

Table 504: *tmnxDhcpSvrLeaseDelete* properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| 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 " <i>\$tmnxDhcpServerCfgServerName\$</i> " ip-address " <i>\$tmnxDhcpSvrLeaseClientAddress\$</i> " client (mac= <i>\$tmnxDhcpSvrNotifMsgHwAddress\$</i> DUID=0x <i>\$tmnxDhcpSvrNotifClientDUID\$</i> configuration deleted |
| Cause | The <code>tmnxDhcpSvrLeaseDelete</code> notification is generated when a DHCP host is deleted. This notification is generated for DHCP server instances with the value of <code>tmnxDhcpServerCfgAddrType</code> set to 'ipv4(1)' or 'ipv6(2)'. |
| Effect | N/A |
| Recovery | N/A |

15.14 tmnxDhcpSvrLeaseModify

Table 505: *tmnxDhcpSvrLeaseModify* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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=\$tmnxDhcpSvrNotifMsgHwAddress\$ DUID=0x\$tmnxDhcpSvrNotifClientDUID\$) configuration modified |
| Cause | The tmnxDhcpSvrLeaseModify notification is generated when a DHCP host is modified. This notification is generated for DHCP server instances with the value of tmnxDhcpServerCfgAddrType set to 'ipv4(1)' or 'ipv6(2)'. |
| Effect | N/A |
| Recovery | N/A |

15.15 tmnxDhcpSvrLeaseNotOwner

Table 506: *tmnxDhcpSvrLeaseNotOwner* properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| 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 |
|---------------|---|
| | <i>LeaseClientAddrLen</i>) is not owned by sender of DHCP message (Hw Addr= <i>\$tmnxDhcpSvrNotifMsgHwAddress</i> , DUID=0x <i>\$tmnxDhcpSvrNotifClientDUID</i>) <i>\$tmnxDhcpSvrNotifDescription</i> |
| Cause | The <i>tmnxDhcpSvrLeaseNotOwner</i> 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 507: *tmnxDhcpSvrMaxLeasesReached* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2010 |
| Event name | <i>tmnxDhcpSvrMaxLeasesReached</i> |
| SNMP notification prefix and OID | TIMETRA-DHCP-SERVER-MIB. <i>tmnxDhcpServerNotifications.10</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | The maximum number of leases (<i>\$tmnxDhcpSvrMaxLeases</i>) has been reached -- dropping DHCP message from sender (mac= <i>\$tmnxDhcpSvrNotifMsgHwAddress</i> DUID=0x <i>\$tmnxDhcpSvrNotifClientDUID</i>) |
| Cause | The <i>tmnxDhcpSvrMaxLeasesReached</i> 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 508: *tmnxDhcpSvrMsgTooLong* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 <i>\$tmnxDhcpSvrNotifServerName\$</i> outgoing message to client (mac= <i>\$tmnxDhcpSvrNotifMsgHwAddress\$</i> , DUID=0x <i>\$tmnxDhcpSvrNotifClientDUID\$</i>) too long (max size= <i>\$tmnxDhcpSvrNotifMsgSizeLimit\$</i>) |
| 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 509: *tmnxDhcpSvrNoContFreeBlocks* properties

| Property name | Value |
|------------------|-------|
| Application name | DHCP |
| 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 510: tmnxDhcpSvrNoSubnetFixAddr properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| 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= <i>\$tmnxDhcpSvrNotifMsgHwAddress\$</i>) |
| Cause | The <i>tmnxDhcpSvrNoSubnetFixAddr</i> 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 <i>tmnxDhcpSvrNoSubnetFixAddr</i> notification is generated, and the request is dropped. This notification is only generated for DHCP server instances with the value of <i>tmnxDhcpServerCfgAddrType</i> set to 'ip4(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 511: *tmnxDhcpSvrPfxThDepletedV6* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2033 |
| Event name | <i>tmnxDhcpSvrPfxThDepletedV6</i> |
| SNMP notification prefix and OID | TIMETRA-DHCP-SERVER-MIB. <i>tmnxDhcpServerNotifications.33</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | No free prefixes with minimum threshold length <i>\$tmnxDhcpsPfxMinFreePrefixLen\$</i> in prefix ' <i>\$tmnxDhcpSvrSubnetAddress\$/\$tmnxDhcpSvrSubnetPrefixLength\$</i> ' in pool ' <i>\$tmnxDhcpServerPoolName\$</i> ' in server ' <i>\$tmnxDhcpServerCfgServerName\$</i> '. |
| Cause | The <i>tmnxDhcpSvrPfxThDepletedV6</i> 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 512: tmnxDhcpSvrPfxThTooLowV6 properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 <i>\$tmnxDhcpSvrPfxMinFreePrefixLen\$</i> in prefix <i>\$tmnxDhcpSvrSubnetAddress\$/\$tmnxDhcpSvrSubnetPrefixLength\$</i> , pool <i>\$tmnxDhcpServerPoolName\$</i> , server <i>\$tmnxDhcpServerCfgServerName\$</i> is becoming low. <i>\$tmnxDhcpSvrPfxThCurrFreeBlksHw\$/\$tmnxDhcpSvrPfxThCurrFreeBlksLw\$</i> free prefix(es). (Minimum free threshold <i>\$tmnxDhcpSvrPfxMinFreePercent\$%/ \$tmnxDhcpSvrPfxMinFreeNumber\$</i>) |
| 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 tmnxDhcpSvrPITHDepletedV6

Table 513: *tmnxDhcpSvrPITHDepletedV6* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2031 |
| Event name | tmnxDhcpSvrPITHDepletedV6 |
| 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 <i>\$tmnxDhcpPIMinFreePrefixLen\$</i> in pool ' <i>\$tmnxDhcpServerPoolName\$</i> ' in server ' <i>\$tmnxDhcpServerCfgServerName\$</i> '. |
| Cause | The tmnxDhcpSvrPITHDepletedV6 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 tmnxDhcpSvrPITHTooLowV6

Table 514: *tmnxDhcpSvrPITHTooLowV6* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2030 |
| Event name | tmnxDhcpSvrPITHTooLowV6 |
| 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 <i>\$tmnxDhcpPfxMinFreePrefixLen\$</i> in pool ' <i>\$tmnxDhcpSvrPoolName\$</i> ', server <i>\$tmnxDhcpServerCfgServerName\$</i> is becoming low. <i>\$tmnxDhcpSPIThCurrFreeBlksHw\$</i> / <i>\$tmnxDhcpSPIThCurrFreeBlksLw\$</i> free prefix(es). (Minimum free threshold <i>\$tmnxDhcpSPIMinFreePercent\$</i> %) |
| Cause | The <i>tmnxDhcpSvrPIThTooLowV6</i> 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 515: *tmnxDhcpSvrPoolDepleted* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| Event ID | 2015 |
| Event name | <i>tmnxDhcpSvrPoolDepleted</i> |
| SNMP notification prefix and OID | TIMETRA-DHCP-SERVER-MIB. <i>tmnxDhcpServerNotifications.15</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | No free addresses in pool " <i>\$tmnxDhcpServerPoolName\$</i> " |
| Cause | The <i>tmnxDhcpSvrPoolDepleted</i> 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 <i>tmnxDhcpServerCfgAddrType</i> set to 'ipv4(1)'. |
| Effect | N/A |
| Recovery | N/A |

15.25 tmnxDhcpSvrPoolMinFreeExc

Table 516: *tmnxDhcpSvrPoolMinFreeExc* properties

| Property name | Value |
|----------------------------------|---|
| Application name | DHCP |
| 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 (<i>\$tmnxDhcpSvrNotifPoolFree\$</i>) has fallen below the desired minimum (<i>\$tmnxDhcpServerPoolMinFree\$</i>) in pool " <i>\$tmnxDhcpServerPoolName\$</i> " |
| 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 517: *tmnxDhcpSvrPoolUnknown* properties

| Property name | Value |
|------------------|------------------------|
| Application name | DHCP |
| 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 <i>\$tmnxDhcpSvrNotifServerName\$</i> detects an unknown pool (<i>\$tmnxDhcpSvrNotifUnknownPoolName\$</i>). <i>\$tmnxDhcpSvrNotifDescription\$</i> sender (mac= <i>\$tmnxDhcpSvrNotifMsgHwAddress\$</i> , DUID=0x <i>\$tmnxDhcpSvrNotifClientDUID\$</i>) |
| 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 518: *tmnxDhcpSvrSubnetDepleted* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 <i>\$tmnxDhcpSvrSubnetAddress\$</i> / <i>\$tmnxDhcpSvrSubnetPrefixLength\$</i> |
| 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 tmnxDhcpServerCfgAddrType set to 'ipv4(1)'. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

15.28 tmnxDhcpSvrSubnetMinFreeExc

Table 519: tmnxDhcpSvrSubnetMinFreeExc properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 (<i>\$tmnxDhcpSvrSubnetStatsFree\$</i>) has fallen below the desired minimum (<i>\$tmnxDhcpSvrSubnetMinFree\$</i>) in subnet <i>\$tmnxDhcpSvrSubnetAddress\$/\$tmnxDhcpSvrSubnetPrefix Length\$</i> |
| 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 520: *tmnxDhcpSvrUserDbUnknown* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 <i>\$tmnxDhcpServerCfgUserDatabase\$</i> specified for server <i>\$tmnxDhcpServerCfgServerName\$</i> does not exist -- dropping DHCP message from sender (mac= <i>\$tmnxDhcpSvrNotifMsgHwAddress\$</i>) |
| 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)'. 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 521: *tmnxLudbDhcpGroupIfTooLong* properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 " \$tmnxLudbNotifyPortId\$" 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 522: tmnxLudbPppoeGroupIfTooLong properties

| Property name | Value |
|----------------------------------|--|
| Application name | DHCP |
| 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 " \$tmnxLudbNotifyPortId\$" is too long. |
| Cause | The tmnxLudbPppoeGroupIfTooLong notification is generated when the default MSAP group interface name concatenated with the port-id is longer than 32 characters. |
| Effect | N/A |
| Recovery | N/A |

16 DIAMETER

16.1 tmnxDiamAppSessionFailure

Table 523: *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= <i>\$tmnxDiamAppSessionId\$</i> , subscrid= <i>\$tmnxDiamAppSubscrid\$</i> , sapid= <i>\$tmnxDiamAppSapId\$</i> , slaprof= <i>\$tmnxDiamAppSLAProfName\$ \$tmnxDiamNotifySpiShare Type\$: \$tmnxDiamNotifySpiShareId\$, \$tmnxDiamAppTrapDescription\$</i> |
| 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 524: *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= <i>\$tmnxDiamPlcyName\$</i> , peer= <i>\$tmnxDiamPeerStatsPeerName\$</i> , client-side-peer-ip= <i>\$tmnxDiamPeerStatsPeerIpAddr\$</i> , tcp-port= <i>\$tmnxDiamPeerStatsPeerPort\$</i> , drop-count= <i>\$tmnxDiamPeerStatsFailedMessages\$</i> , <i>\$tmnxDiamAppTrapDescription\$</i> |
| Cause | The tmnxDiamMessageDropped notification indicates that the DIAMETER protocol has dropped a message. |
| Effect | N/A |
| Recovery | N/A |

16.3 tmnxDiamNdPeerStatActiveChanged

Table 525: 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 <i>\$tmnxDiamNodeOriginHost\$</i> , peer <i>\$tmnxDiamNodeDestinationHost\$</i> is <i>\$tmnxDiamNdPeerStatActive\$</i> 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 526: *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 <i>\$tmnxDiamPlcyName\$</i> , peer <i>\$tmnxDiamPlcyPeer Name\$</i> now has operational state: PrimarySecondary = <i>\$tmnxDiam PeerPrimarySecondary\$</i> , connectionSuspended = <i>\$tmnxDiamPeer ConnectionSuspended\$</i> and cooldownSeqActive = <i>\$tmnxDiamPeer CooldownSeqActive\$</i> , <i>\$tmnxDiamAppTrapDescription\$</i> |
| Cause | The state of the diameter policy peer changed. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

16.5 tmnxDiamPpPrxMcLocStateChanged

Table 527: *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 <i>\$tmnxDiamPpPrxMcLocState\$</i> changed to <i>\$tmnxDiamPpPrxMcLocState\$</i> |
| 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 528: *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=' <i>\$tmnxDiamAppSessionId\$</i> ', policy=' <i>\$tmnxDiamAppPlcyId\$</i> ', application= <i>\$tmnxDiamAppPlcyApplication\$</i> , event= <i>\$tmnxDiamNotifyEventId\$</i> , <i>\$tmnxDiamAppTrapDescription\$</i> |
| Cause | A Diameter session has experienced a problem. The session ID is indicated with the <i>tmnxDiamAppSessionId</i> . The associated Diameter application policy is indicated with the <i>tmnxDiamAppPlcyApplication</i> . What happened is indicated with the <i>tmnxDiamNotifyEventId</i> and the <i>tmnxDiamAppTrapDescription</i> . |
| 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 529: *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 <i>\$alxDot1xNotifyMacAddress\$</i> port <i>\$alxDot1xNotifyPort\$</i> authentication <i>\$alxDot1xNotifyAuthHostEvent\$</i> <i>\$alxDot1xNotifyDescription\$</i> |
| 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 <i>alxDot1xNotifyDescription</i> may contain additional information. |
| Recovery | Recovery, if any, depends on the particular event. |

18 DYNSVC

18.1 tmnxDynSvcSapFailed

Table 530: 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 <i>\$tmnxDynSvcNotifSapAcctSessionId\$</i> (SAP <i>\$tmnxDynSvcNotifSapPortId\$</i>) could not be completed - <i>\$tmnxDynSvcNotifDescription\$</i> |
| 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 531: 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 <i>\$ifIndex\$</i> raised <i>\$dot3OamEventLogLocation\$</i> fault <i>\$dot3OamEventLogType\$</i> |
| 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 532: 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 <i>\$ifIndex\$</i> raised <i>\$dot3OamEventLogLocation\$</i> SF fault <i>\$dot3OamEventLogType\$</i> - <i>\$dot3OamEventLogValue\$</i> errors exceeded the <i>\$dot3OamEventLogThresholdLo\$</i> error threshold during the <i>\$dot3OamEventLogWindowLo\$</i> 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 533: 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 <i>\$subject\$</i> |
| 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 534: *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 <i>\$subject\$</i> |
| 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 535: *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 <i>\$ifIndex\$</i> cleared <i>\$dot3OamEventLogLocation\$</i> fault <i>\$dot3OamEventLogType\$</i> |
| 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 536: *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 <i>\$subject\$</i> has changed to <i>\$dot3OamPeerMacAddress\$</i> |

| 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 537: 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 <i>\$ifIndex\$</i> <i>\$tmnxDot3OamSdEventLogCleared\$</i> <i>\$tmnxDot3OamSdEventLogLocation\$</i> SD fault <i>\$tmnxDot3OamSdEventLogType\$</i> - <i>\$tmnxDot3OamSdEventLogValue\$</i> errors exceeded the <i>\$tmnxDot3OamEventLogSdThresholdLo\$</i> error threshold during the <i>\$tmnxDot3OamSdEventLogWindowLo\$</i> <i>\$tmnxDot3OamSdEventLogType\$</i> 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 538: *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 <i>\$ifIndex\$</i> cleared <i>\$dot3OamEventLogLocation\$</i> SF fault <i>\$dot3OamEventLogType\$</i> - <i>\$dot3OamEventLogValue\$</i> errors exceeded the <i>\$dot3OamEventLogThresholdLo\$</i> error threshold during the <i>\$dot3OamEventLogWindowLo\$</i> <i>\$dot3OamEventLogType\$</i> 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 539: 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 tmnxElmilfCfgMode is set to 'none (0)'." |
| Effect | N/A |
| Recovery | N/A |

20.2 tmnxElmilfStatusChangeEvent

Table 540: tmnxElmilfStatusChangeEvent properties

| Property name | Value |
|------------------|-------|
| Application name | ELMI |
| Event ID | 2001 |

| Property name | Value |
|----------------------------------|---|
| Event name | tmnxElmilfStatusChangeEvent |
| SNMP notification prefix and OID | TIMETRA-ELMI-MIB.tmnxElmiNotifications.1 |
| Default severity | minor |
| Source stream | main |
| Message format string | ELMI on <i>\$tmnxPortPortID\$</i> has changed status to <i>\$tmnxElmilfCfg Status\$</i> |
| 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 541: *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 <i>\$tmnxEthRingIndex\$</i> 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 542: *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 <i>\$tmnxEthRingIndex\$</i> provisioning mismatch (FOP-PM) detected: RPL blocked in Node <i>\$node\$</i> |
| 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 543: *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 <i>\$tmnxEthRingIndex\$</i> path <i>\$tmnxEthRingPathIndex\$</i> changed fwd state to <i>\$tmnxethRingPathFwdState\$</i> |
| 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 544: 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 <i>\$dot1agCfmMdIndex\$</i> / <i>\$dot1agCfmMaIndex\$</i> / <i>\$dot1agCfmMepIdentifier\$</i> highest defect is now <i>\$dot1agCfmMepHighestPrDefect\$</i> |
| 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 dot1agCfmMepHighestPrDefect variable in the notification: dot1agCfmMdIndex - Also the index of the MEP's Maintenance Domain table entry (dot1agCfmMdTable). dot1agCfmMaIndex - Also an index (with the MD table index) of the MEP's Maintenance Association network table entry (dot1agCfmMaNetTable), and (with the MD table index and component ID) of the MEP's MA component table entry (dot1agCfmMaCompTable). dot1agCfmMepIdentifier - 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 545: 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 <i>\$dot1agCfmMdlIndex\$</i> / <i>\$dot1agCfmMlIndex\$</i> / <i>\$dot1agCfmMepIdentifier\$</i> |
| 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 546: 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: <ul style="list-style-type: none"> MEP <i>\$dot1agCfmMdIndex\$/ \$dot1agCfmMaIndex\$/ \$dot1agCfmMepIdentifier\$</i> is clear of CSF state MEP <i>\$dot1agCfmMdIndex\$/ \$dot1agCfmMaIndex\$/ \$dot1agCfmMepIdentifier\$</i> is in CSF state |
| Cause | The <i>tmnxDot1agCfmMepCsfStateChanged</i> notification is generated when a MEP enters or exits a CSF state. |
| Effect | N/A |
| Recovery | N/A |

22.4 tmnxDot1agCfmMepDMTestComplete

Table 547: *tmnxDot1agCfmMepDMTestComplete* properties

| Property name | Value |
|----------------------------------|--|
| Application name | ETH_CFM |
| Event ID | 2005 |
| Event name | <i>tmnxDot1agCfmMepDMTestComplete</i> |
| SNMP notification prefix and OID | TIMETRA-IEEE8021-CFM-MIB. <i>tmnxDot1agNotifications.4</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | <i>\$tmnxDot1agCfmMepDelayTestType\$</i> test complete on MEP <i>\$dot1agCfmMdIndex\$/ \$dot1agCfmMaIndex\$/ \$dot1agCfmMepIdentifier\$</i> : Delay= <i>\$tmnxDot1agCfmMepDelayTestDelay\$</i> us |
| Cause | The <i>tmnxDot1agCfmMepDMTestComplete</i> 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 548: 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 <i>\$dot1agCfmMdlIndex\$/\$dot1agCfmMlIndex\$/\$dot1agCfmMepIdentifier\$</i> : Bytes/Failed Bits/CRC Failures= <i>\$tmnxDot1agCfmMepCurrByteCount\$/\$tmnxDot1agCfmMepCurrFailedBits\$/\$tmnxDot1agCfmMepCurrCrcFailures\$</i> |
| Cause | The tmnxDot1agCfmMepEthTestComplete notification indicates that an eth-test has been issued and results are ready. The tmnxDot1agCfmMepCurrByteCount 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 549: 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 <i>\$tmnxDot1agCfmMepFcltyType\$</i> <i>\$tmnxDot1agCfmMepFcltyInstance\$</i> |
| 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 550: 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 <i>\$tmnxDot1agCfmMepFcltyType\$</i> <i>\$tmnxDot1agCfmMepFcltyInstance\$</i> |
| 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 551: 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 <i>\$dot1agCfmMdIndex\$</i> / <i>\$dot1agCfmMaIndex\$</i> / <i>\$dot1agCfmMepIdentifier\$</i> for <i>\$dot1agCfmMepTransmitLbmDestMacAddress\$</i> are available (MEP admin-name = " <i>\$tmnxDot1agCfmMdAdminName\$</i> "/ <i>\$tmnxDot1agCfmMaNetAdminName\$</i> / <i>\$dot1agCfmMepIdentifier\$</i>) |
| 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 552: *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 <i>\$dot1agCfmMepTransmitLtmSeqNumber\$</i> on MEP <i>\$dot1agCfmMdIndex\$/\$dot1agCfmMaIndex\$/\$dot1agCfmMepIdentifier\$</i> are now available (MEP admin-name = " <i>\$tmnxDot1agCfmMdAdminName\$</i> "/ <i>\$tmnxDot1agCfmMaNetAdminName\$</i> "/ <i>\$dot1agCfmMepIdentifier\$</i>) |
| 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 553: *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 <i>\$tmnxDot1agCfmMepMonitorOperGrp\$</i> changed MEP <i>\$dot1agCfmMdIndex\$/ \$dot1agCfmMaIndex\$/ \$dot1agCfmMepIdentifier\$</i> state to <i>\$tmnxDot1agCfmMepOperGrpState\$</i> |
| Cause | The <i>tmnxDot1agCfmMepOperGrpStateChgd</i> notification is generated when there is a change in the value of <i>tmnxDot1agCfmMepOperGrpState</i> . |
| 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 554: *tmnxDot1agCfmMepSLMTestComplete* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ETH_CFM |
| Event ID | 2008 |
| Event name | <i>tmnxDot1agCfmMepSLMTestComplete</i> |
| SNMP notification prefix and OID | TIMETRA-IEEE8021-CFM-MIB. <i>tmnxDot1agNotifications.7</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | SLM <i>\$tmnxDot1agCfmMepSlmTestType\$</i> (test-id <i>\$tmnxDot1agCfmMepSlmTestId\$</i>) completed for remote-mep <i>\$tmnxDot1agCfmMepSlmRemoteMepId\$</i> remote MAC <i>\$tmnxDot1agCfmMepSlmRemoteMacAddr\$</i> |
| Cause | The <i>tmnxDot1agCfmMepSLMTestComplete</i> notification is generated when a one-way or two-way Synthetic Loss Measurement (SLM) test is completed. For one-way SLM test results, <i>tmnxDot1agCfmMepSlmPacketLossOut</i> and <i>tmnxDot1agCfmMepSlmPacketUnack</i> values are fixed at 'zero(0)'. |
| Effect | N/A |
| Recovery | N/A |

22.12 tmnxDot1agCfmMipEvaluation

Table 555: *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 <i>\$tmnxDot1agCfmNotifySvcId\$</i> 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 556: *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 <i>\$tmnxEthTunnelIndex\$</i> cleared configuration mismatch <i>\$tmnxEthTunnelApsDefectStatus\$</i> |
| 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 557: *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 <i>\$tmnxEthTunnelIndex\$</i> experiencing configuration mismatch <i>\$tmnxEthTunnelApsDefectStatus\$</i> |
| 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 558: *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 <i>\$tmnxEthTunnelIndex\$</i> cleared incomplete protection switch (<i>\$tmnxEthTunnelApsDefectStatus\$</i>) |
| Cause | The tmnxEthTunnelApsNoRspClearAlarm is generated when an Ethernet Tunnel Group no longer experiences an incompleteness of protection switching at the ETH layer. |
| Effect | N/A |
| Recovery | N/A |

23.4 tmnxEthTunnelApsNoRspRaiseAlarm

Table 559: *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 <i>\$tmnxEthTunnelIndex\$</i> experiencing incomplete protection switch (<i>\$tmnxEthTunnelApsDefectStatus\$</i>) |
| Cause | The tmnxEthTunnelApsNoRspRaiseAlarm is generated when an Ethernet Tunnel Group experiences an incompleteness 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 560: *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 <i>\$tmnxEthTunnelIndex\$</i> cleared provisioning mismatch <i>\$tmnxEthTunnelApsDefectStatus\$</i> (<i>\$tmnxEthTunnelApsRxPdu\$</i> / <i>\$tmnxEthTunnelApsTxPdu\$</i>) |
| Cause | The tmnxEthTunnelApsPrvsnClearAlarm is generated when an Ethernet Tunnel Group provisioning mismatch is cleared. |
| Effect | N/A |
| Recovery | N/A |

23.6 tmnxEthTunnelApsPrvsnRaiseAlarm

Table 561: 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 <i>\$tmnxEthTunnelIndex\$</i> experiencing provisioning mismatch <i>\$tmnxEthTunnelApsDefectStatus\$</i> : Rx 0x <i>\$tmnxEthTunnelApsRxPdu\$</i> Tx 0x <i>\$tmnxEthTunnelApsTxPdu\$</i> |
| 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 562: *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 <i>\$tmnxEthTunnelIndex\$</i> experienced member activity switchover. Path <i>\$tmnxEthTunnelMemberIndex\$</i> 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 563: 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 <i>\$tFiltrPrefixListType\$</i> prefix-list <i>\$tFiltrPrefixListName\$</i> for apply-path <i>\$tFiltrApplyPathSource\$ \$tFiltrApplyPathIndex\$: \$tFilterAlarmDescription\$</i> |
| 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 564: 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 565: 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 <i>\$tFilterEmbeddedRefEmbeddedFiltrId\$</i> in the embedding filter <i>\$tFilterEmbeddedRefFilterType\$</i> ID <i>\$tFilterEmbeddedRefInsertFiltrId\$</i> has changed to <i>\$tFilterEmbeddedRefOperState\$</i> . |
| 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 566: 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 <i>\$tFilterEmbedFlowspecRtrId\$</i> in the embedding filter <i>\$tFilterEmbedFlowspecFilterType\$</i> ID <i>\$tFilterEmbedFlowspecInsertFtrId\$</i> has changed to <i>\$tFilterEmbedFlowspecOperState\$</i> . |
| 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 567: 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 <i>\$tFilterEmbedOpenflowOfsName\$</i> in the embedding filter <i>\$tFilterEmbedOpenflowFilterType\$</i> ID <i>\$tFilterEmbedOpenflowInsertFtrId\$</i> has changed to <i>\$tFilterEmbedOpenflowOperState\$</i> . |
| 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 568: 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 <i>\$ftrOpenFlowFlowEntryId\$</i> for the open-flow flowTable <i>\$ftrOpenFlowFlowTable\$</i> . Additional Info: <i>\$ftrOpenFlowProblemDescription\$</i> . |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

24.7 tFilterRadSharedFltrAlarmClear

Table 569: 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 <i>\$tFilterType\$ \$tFilterId\$</i> has dropped below the threshold of <i>\$tFilterThresholdReached\$</i> |
| 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 570: 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 <i>\$tFilterType\$ \$tFilterId\$</i> has exceeded its threshold of <i>\$tFilterThresholdReached\$</i> |
| 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 571: 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 <i>\$tFilterRedirectPolicy\$</i> has changed to <i>\$tFilterRPActiveDestAddr\$</i> . |
| 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 572: 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 <i>\$tFilterType\$ \$tFilterId\$</i> for <i>\$tFilterSubInsSpaceOwner\$</i> has failed - <i>\$tFilterAlarmDescription\$</i> |
| 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 573: 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 <i>\$tFilterType\$ \$tFilterId\$</i> for <i>\$tFilterSubInsSpaceOwner\$</i> has fallen below its configured low watermark level <i>\$tFilterThresholdReached\$</i> |
| 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 574: *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 <i>\$tFilterType\$ \$tFilterId\$</i> for <i>\$tFilterSub InsSpaceOwner\$</i> is filled up to its configured high watermark level <i>\$t FilterThresholdReached\$</i> |
| 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 575: *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 <i>\$tIPFilterId\$</i> entry <i>\$tIPFilterParamsIndex\$</i> PBR packets dropped on interface <i>\$tIPFilterParamsForwardNHInterface\$</i> because <i>\$tFilterPBRDropReason\$</i> . |
| Cause | The tIPFilterPlyBasedRoutingPacketsDrop 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 tIPFilterPlyBasedRoutingPacketsDrop 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 576: *tmnxAncpEgrRateMonitorEvent* properties

| Property name | Value |
|----------------------------------|---|
| Application name | GSMP |
| Event ID | 2003 |
| Event name | tmnxAncpEgrRateMonitorEvent |
| SNMP notification prefix and OID | TIMETRA-GSMP-MIB.tmnxGsmNotifications.2 |
| Default severity | warning |
| Source stream | main |
| Message format string | The Egress rate monitor function for the port identified by <i>\$tmnxNotifAncpString\$</i> detects that the scheduler rate <i>\$tmnxNotifAncpPlcyActualRate\$</i> has dropped below the value specified by <i>\$tmnxNotifAncpPolicyName\$</i> |
| Cause | This notification is generated when the egress rate monitor function for the port identified by <i>tmnxAncpString</i> detects that the scheduler rate has dropped below <i>tmnxAncpPlcyEgrRateMonitor</i> . |
| 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 577: *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 <i>\$tmnxNotifAncpString\$</i> detects that the scheduler rate <i>\$tmnxNotifAncpPlcyActualRate\$</i> has dropped below the value specified by <i>\$tmnxNotifAncpPolicyName\$</i> |
| Cause | This notification is generated when the egress rate monitor function for the port identified by <i>tmnxAncpString</i> detects that the scheduler rate has dropped below <i>tmnxAncpPlcyEgrRateMonitor</i> . |
| 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 tmnxAncpIngrRateMonitorEvent

Table 578: *tmnxAncpIngrRateMonitorEvent* properties

| Property name | Value |
|----------------------------------|--|
| Application name | GSMP |
| Event ID | 2001 |
| Event name | tmnxAncpIngrRateMonitorEvent |
| SNMP notification prefix and OID | TIMETRA-GSMP-MIB.tmnxGsmNotifications.1 |
| Default severity | warning |
| Source stream | main |
| Message format string | The ingress rate monitor function for the port identified by <i>\$tmnxNotifAncpString\$</i> detects that the scheduler rate <i>\$tmnxNotifAncpPlcyActualRate\$</i> has dropped below the value specified by <i>\$tmnxNotifAncpPolicyName\$</i> |

| Property name | Value |
|---------------|--|
| Cause | This notification is generated whenever the ingress rate monitor function for the port identified by <code>tmnxAncpString</code> detects that the scheduler rate has dropped below <code>tmnxAncpPlcyIngRateMonitor</code> . |
| 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. |

25.4 `tmnxAncpIngRateMonitorEventL`

Table 579: `tmnxAncpIngRateMonitorEventL` properties

| Property name | Value |
|----------------------------------|--|
| Application name | GSMP |
| Event ID | 2002 |
| Event name | <code>tmnxAncpIngRateMonitorEventL</code> |
| 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 <code>\$tmnxNotifAncpString\$</code> detects that the scheduler rate <code>\$tmnxNotifAncpPlcyActualRate\$</code> has dropped below the value specified by <code>\$tmnxNotifAncpPolicyName\$</code> |
| Cause | This notification is generated when the ingress rate monitor function for the port identified by <code>tmnxAncpString</code> detects that the scheduler rate has dropped below <code>tmnxAncpPlcyIngRateMonitor</code> . |
| 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 580: *tmnxAncpSesRejected* properties

| Property name | Value |
|----------------------------------|--|
| Application name | GSMP |
| Event ID | 2007 |
| Event name | tmnxAncpSesRejected |
| SNMP notification prefix and OID | TIMETRA-GSMP-MIB.tmnxGsmNotifications.4 |
| Default severity | warning |
| Source stream | main |
| Message format string | An incoming ANCP session has been rejected: <i>\$tmnxAncpRejectReason\$</i> |
| 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 581: *tmnxAncpShcvDisabledEvent* properties

| Property name | Value |
|----------------------------------|--|
| Application name | GSMP |
| Event ID | 2005 |
| Event name | tmnxAncpShcvDisabledEvent |
| SNMP notification prefix and OID | TIMETRA-GSMP-MIB.tmnxGsmNotifications.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 <i>\$tmnxNotifAncpString\$</i> when a port-down event was received. AncpPolicy: <i>\$tmnxNotifAncpPolicyName\$</i> |

| 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 582: 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 <i>\$tmnxNotifAncpString\$</i> when a port-down event was received. AncpPolicy: <i>\$tmnxNotifAncpPolicyName\$</i> |
| 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 583: *tmnxAncpStringRejected* properties

| Property name | Value |
|----------------------------------|---|
| Application name | GSMP |
| Event ID | 2008 |
| Event name | tmnxAncpStringRejected |
| SNMP notification prefix and OID | TIMETRA-GSMP-MIB.tmnxGsmNotifications.5 |
| Default severity | warning |
| Source stream | main |
| Message format string | An incoming ANCP string rejected: <i>\$tmnxAncpRejectReason\$</i> |
| 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 tmnxAncpRejectReason. |
| Effect | The ANCP string is rejected. |
| Recovery | No recovery is necessary. |

26 IGMP

26.1 vRtrIgmPGrpIfSapCModeRxQueryMism

Table 584: 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 (<i>\$vRtrIgmPGrpIfSapOperVersion</i>) for SAP <i>\$sapPortId</i> on interface <i>\$vRtrGrpIfIndex</i> , IGMP instance <i>\$vRtrID</i> , and the IGMP query version (<i>\$vRtrIgmPNotifyQueryVersion</i>) 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. vRtrIgmPGrpIfSapOperVersion 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 585: 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 <i>\$sapPortId\$</i> on interface <i>\$vRtrGrpIfIndex\$</i> , IGMP instance <i>\$vRtrID\$</i> , has exceeded the maximum limit of <i>\$vRtrIgmPGrpIfSapMaxGroups\$</i> |
| 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 vRtrIgmPGrpIfSapMaxGroups, the maximum number of groups supported on the system. |
| Effect | N/A |
| Recovery | N/A |

26.3 vRtrIgmPGrpIfSapMaxGrpSrcLimExcd

Table 586: 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 <i>\$sapPortId\$</i> on interface <i>\$vRtrGrpIfIndex\$</i> , IGMP instance <i>\$vRtrID\$</i> , has exceeded the maximum limit of <i>\$vRtrIgmPGrpIfSapMaxSources\$</i> |
| Cause | The <i>vRtrIgmPGrpIfSapMaxGrpSrcLimExcd</i> 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 <i>vRtrIgmPGrpIfSapMaxGrpSources</i> , the maximum number of group sources per group supported on the SAP. |
| Effect | N/A |
| Recovery | N/A |

26.4 vRtrIgmPGrpIfSapMaxSrcsLimExceed

Table 587: *vRtrIgmPGrpIfSapMaxSrcsLimExceed* properties

| Property name | Value |
|----------------------------------|---|
| Application name | IGMP |
| Event ID | 2013 |
| Event name | <i>vRtrIgmPGrpIfSapMaxSrcsLimExceed</i> |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB. <i>vRtrIgmPNotifications.13</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | The number of sources for SAP <i>\$sapPortId\$</i> on interface <i>\$vRtrGrpIfIndex\$</i> , IGMP instance <i>\$vRtrID\$</i> , has exceeded the maximum limit of <i>\$vRtrIgmPGrpIfSapMaxSources\$</i> |
| Cause | The <i>vRtrIgmPGrpIfSapMaxSrcsLimExceed</i> 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 <i>vRtrIgmPGrpIfSapMaxSources</i> , the maximum number of sources per group supported on the system. |
| Effect | N/A |
| Recovery | N/A |

26.5 vRtrIgmPGrpIfSapMcacPlcyDropped

Table 588: 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 <i>\$vRtrIgmPNotifyGrpAddr\$</i> is dropped because of MCAC policy <i>\$vRtrIgmPNotifyMcacPolicyName\$</i> for SAP <i>\$sapPortId\$</i> on interface <i>\$vRtrGrpIfIndex\$</i> , IGMP instance <i>\$vRtrID\$</i> |
| 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 589: 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\$ <i>vRtrIgmPNotifyQueryVersion</i> \$ query received for SAP \$ <i>sapPortId</i> \$ on interface \$ <i>vRtrGrpIfIndex</i> \$, IGMP instance \$ <i>vRtrID</i> \$, configured as IGMPv\$ <i>vRtrIgmPGrpIfSapAdminVersion</i> \$ |
| Cause | A <i>vRtrIgmPGrpIfSapRxQueryVerMism</i> notification is generated when the IGMP host SAP is configured as IGMPv3 but receives a IGMPv1 Query or IGMPv2 General Query on the host. <i>sapPortId</i> and <i>sapEncapValue</i> will identify the SAP on which the query is received. <i>vRtrIgmPGrpIfSapAdminVersion</i> will contain the configured version of the SAP and <i>vRtrIgmPNotifyQueryVersion</i> will contain the version of the received query. |
| Effect | N/A |
| Recovery | N/A |

26.7 vRtrIgmPHostCModeRxQueryMismatch

Table 590: *vRtrIgmPHostCModeRxQueryMismatch* properties

| Property name | Value |
|----------------------------------|--|
| Application name | IGMP |
| Event ID | 2008 |
| Event name | <i>vRtrIgmPHostCModeRxQueryMismatch</i> |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB. <i>vRtrIgmPNotifications</i> .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 591: 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 592: 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 <i>\$vRtrIgmppGrpIffHostLastChangeTime\$ - \$vRtrIgmppNotifyDescription\$</i> |
| Cause | The vRtrIgmppMaxGrpsLimitExceeded event is generated when an attempt is made to configure a group when vRtrIgmppHostGroupCount, the number of groups configured on the PIM interface, is equal to vRtrIgmppHostMaxGroups, the maximum number of groups supported on the system. |
| Effect | None. |
| Recovery | Contact Nokia Customer Service. |

26.10 vRtrIgmppHostMaxGrpSrcsLimitExcd

Table 593: vRtrIgmppHostMaxGrpSrcsLimitExcd properties

| Property name | Value |
|----------------------------------|---|
| Application name | IGMP |
| Event ID | 2017 |
| Event name | vRtrIgmppHostMaxGrpSrcsLimitExcd |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB.vRtrIgmppNotifications.17 |
| Default severity | minor |
| Source stream | main |
| Message format string | The number of groups or sources configured has exceeded the maximum limit of <i>\$vRtrIgmppHostMaxSources\$</i> |
| Cause | The vRtrIgmppHostMaxGrpSrcsLimitExcd event is generated when an attempt is made to configure a source for a group when the number of group sources is equal to vRtrIgmppHostMaxGrpSources, the maximum number of group sources per group supported on the host. |
| Effect | N/A |
| Recovery | N/A |

26.11 vRtrIgmPHostMaxSrcsLimitExceeded

Table 594: 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 <i>\$vRtrIgmPHostMaxSources\$</i> |
| 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 595: 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 596: 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 Grplf 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 597: vRtrIgmphostRxQueryVerMismatch properties

| Property name | Value |
|----------------------------------|---|
| Application name | IGMP |
| Event ID | 2009 |
| Event name | vRtrIgmphostRxQueryVerMismatch |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB.vRtrIgmphostNotifications.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 vRtrIgmplfCModeRxQueryMismatch

Table 598: vRtrIgmplfCModeRxQueryMismatch properties

| Property name | Value |
|----------------------------------|--|
| Application name | IGMP |
| Event ID | 2002 |
| Event name | vRtrIgmplfCModeRxQueryMismatch |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB.vRtrIgmphostNotifications.2 |
| Default severity | warning |
| Source stream | main |
| Message format string | Mismatch between the interface <i>\$vRtrIfIndex\$</i> compatible mode(<i>\$vRtrIgmplfOperVersion\$</i>) and the version of the IGMP query (version <i>\$vRtrIgmphostNotifyQueryVersion\$</i>) 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 vRtrIgmplfRxQueryVerMismatch

Table 599: vRtrIgmplfRxQueryVerMismatch properties

| Property name | Value |
|----------------------------------|--|
| Application name | IGMP |
| Event ID | 2001 |
| Event name | vRtrIgmplfRxQueryVerMismatch |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB.vRtrIgmplfRxQueryVerMismatch.1 |
| Default severity | warning |
| Source stream | main |
| Message format string | IGMPv\$vRtrIgmplfRxQueryVerMismatch\$ query received on interface \$vRtrIgmplfRxQueryVerMismatch\$ configured as IGMPv\$vRtrIgmplfRxQueryVerMismatch\$ |
| 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 vRtrIgmplfMaxGrpsLimitExceeded

Table 600: vRtrIgmplfMaxGrpsLimitExceeded properties

| Property name | Value |
|------------------|--------------------------------|
| Application name | IGMP |
| Event ID | 2003 |
| Event name | vRtrIgmplfMaxGrpsLimitExceeded |

| 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 <i>\$ifName\$</i> has exceeded the maximum limit of <i>\$vRtrIgmPlfMaxGroups\$</i> |
| 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 601: 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 <i>\$vRtrIgmPlfMaxSources\$</i> |
| 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 vRtrIgmPlfMaxGrpSources, the maximum number of group sources per group supported on the interface. |
| Effect | N/A |
| Recovery | N/A |

26.19 vRtrIgmPMaxSrcsLimitExceeded

Table 602: 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 $\$vRtrIgmPlfMaxSources\$\$ |
| 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 603: 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 <i>\$vRtrIgmPNotifyGrpAddress\$</i> is dropped because of multicast CAC policy <i>\$vRtrIgmPIfMcacPolicyName\$</i> on interface <i>\$ifName\$</i> IGMP instance <i>\$vRtrID\$</i> |
| Cause | The vRtrIgmPmCacPlyDropped 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 604: 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 <i>\$vRtrIgmPNotifyNumOfIPsecIf\$</i> and has almost reached the maximum value <i>\$vRtrIgmPNotifyMaxNumOfIPsecIf\$</i> . |
| 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 605: 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 <i>\$vRtrIgmPNotifyNumOfIPsecIf\$</i> 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 606: 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 <i>\$vRtrIgmPNotifyMaxNumOfIPsecIf\$</i> . |
| Cause | A <i>vRtrIgmPNotifyNumOfIPsecIfMaxRch</i> 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 vRtrIgmPSlaProfInstMcacPlyDrop

Table 607: vRtrIgmPSlaProfInstMcacPlyDrop properties

| Property name | Value |
|----------------------------------|---|
| Application name | IGMP |
| Event ID | 2024 |
| Event name | vRtrIgmPSlaProfInstMcacPlyDrop |
| SNMP notification prefix and OID | TIMETRA-IGMP-MIB.vRtrIgmPNotifications.24 |
| Default severity | warning |
| Source stream | main |
| Message format string | IGMP group/source <i>\$vRtrIgmPNotifyGrpAddr\$/\$vRtrIgmPNotifySrcAddr\$</i> dropped for SLA profile instance subscriber <i>\$tmnxSubIdent\$</i> SAP <i>\$sapNotifyEncapValue\$</i> SLA profile <i>\$tmnxSubNotifSLAProfName\$</i> group <i>\$tmnxSubNotifSpiGroupId\$</i> due to of MCAC policy <i>\$vRtrIgmPNotifyMcacPolicyName\$</i> instance <i>\$vRtrID\$</i> , reason <i>\$vRtrIgmPNotifyDescription\$</i> |
| Cause | The vRtrIgmPSlaProfInstMcacPlyDrop event is generated when an IGMP group is dropped on a given SLA profile instance because of applying the multicast CAC policy given by vRtrIgmPNotifyMcacPolicy Name. |
| 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 eMplsIcmpSnpGmfibFailure

Table 608: eMplsIcmpSnpGmfibFailure properties

| Property name | Value |
|----------------------------------|--|
| Application name | IGMP_SNOOPING |
| Event ID | 2010 |
| Event name | eMplsIcmpSnpGmfibFailure |
| SNMP notification prefix and OID | ALCATEL-IGMP-SNOOPING-MIB.alxIcmpSnpGEMplsNotifications.1 |
| Default severity | minor |
| Source stream | main |
| Message format string | Failing to store an entry in the MFIB table for service \$svclD |
| Cause | The eMplsIcmpSnpGmfibFailure 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 sapIcmpSnpGGrpLimitExceeded

Table 609: sapIcmpSnpGGrpLimitExceeded properties

| Property name | Value |
|------------------|-----------------------------|
| Application name | IGMP_SNOOPING |
| Event ID | 2001 |
| Event name | sapIcmpSnpGGrpLimitExceeded |

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | ALCATEL-IGMP-SNOOPING-MIB.alxlgmpSnpGsapNotifications.1 |
| Default severity | warning |
| Source stream | main |
| Message format string | The number of groups on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> has exceeded the maximum limit of <i>\$saplgmpSnpGCfgMaxNbrGrps\$</i> - Dropping group <i>\$alxlgmpSnpGGroupAddress\$</i> |
| Cause | The saplgmpSnpGGrpLimitExceeded notification is generated when an IGMP group is dropped on a given SAP because a user configurable upper limit given by saplgmpSnpGCfgMaxNbrGrps is reached. |
| Effect | None. |
| Recovery | Investigate the cause of the excessive groups. |

27.3 saplgmpSnpGGrpSrcLimitExceeded

Table 610: saplgmpSnpGGrpSrcLimitExceeded properties

| Property name | Value |
|----------------------------------|--|
| Application name | IGMP_SNOOPING |
| Event ID | 2009 |
| Event name | saplgmpSnpGGrpSrcLimitExceeded |
| SNMP notification prefix and OID | ALCATEL-IGMP-SNOOPING-MIB.alxlgmpSnpGsapNotifications.5 |
| Default severity | minor |
| Source stream | main |
| Message format string | The number of groups or sources on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> has exceeded the maximum limit of <i>\$saplgmpSnpGCfgMaxNbrSrcs\$</i> - Dropping source <i>\$alxlgmpSnpGSourceAddress\$</i> for group <i>\$alxlgmpSnpGGroupAddress\$</i> |
| Cause | The saplgmpSnpGGrpSrcLimitExceeded notification is generated when an IGMP group or source is dropped on a given SAP because a user configurable upper limit given by saplgmpSnpGCfgMaxNbrGrpSrcs is reached. |
| Effect | The specified S,G was not added. |

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

27.4 saplgmpSnpGMcacPlcyDropped

Table 611: saplgmpSnpGMcacPlcyDropped properties

| Property name | Value |
|----------------------------------|--|
| Application name | IGMP_SNOOPING |
| Event ID | 2002 |
| Event name | saplgmpSnpGMcacPlcyDropped |
| SNMP notification prefix and OID | ALCATEL-IGMP-SNOOPING-MIB.alxlgmpSnpG SapNotifications.2 |
| Default severity | warning |
| Source stream | main |
| Message format string | Group <i>\$alxlgmpSnpGGroupAddress\$</i> is dropped because of multicast CAC policy <i>\$saplgmpSnpG CfgMcacPolicyName\$</i> on SAP <i>\$sapEncap Value\$</i> in service <i>\$svclId\$</i> |
| Cause | The saplgmpSnpGMcacPlcyDropped notification is generated when an IGMP group is dropped on a given SAP because of applying a multicast CAC policy given by saplgmpSnpG CfgMcacPolicyName. |
| Effect | None. |
| Recovery | Investigate the cause of the excessive groups. |

27.5 saplgmpSnpGMcsFailure

Table 612: saplgmpSnpGMcsFailure properties

| Property name | Value |
|------------------|-----------------------|
| Application name | IGMP_SNOOPING |
| Event ID | 2005 |
| Event name | saplgmpSnpGMcsFailure |

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | ALCATEL-IGMP-SNOOPING-MIB.alxlgmpSnpGsapNotifications.3 |
| Default severity | warning |
| Source stream | main |
| Message format string | Group <i>\$alxlgmpSnpGGroupAddress\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> could not be synced to MCS - <i>\$alxlgmpSnpGMcsFailureReason\$</i> |
| Cause | The saplgmpSnpGMcsFailure 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 saplgmpSnpGsrcLimitExceeded

Table 613: saplgmpSnpGsrcLimitExceeded properties

| Property name | Value |
|----------------------------------|---|
| Application name | IGMP_SNOOPING |
| Event ID | 2006 |
| Event name | saplgmpSnpGsrcLimitExceeded |
| SNMP notification prefix and OID | ALCATEL-IGMP-SNOOPING-MIB.alxlgmpSnpGsapNotifications.4 |
| Default severity | warning |
| Source stream | main |
| Message format string | The number of sources for group <i>\$alxlgmpSnpGGroupAddress\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> has exceeded the maximum limit of <i>\$saplgmpSnpGCfgMaxNbrSrcs\$</i> - Dropping source <i>\$alxlgmpSnpGSourceAddress\$</i> for group <i>\$alxlgmpSnpGGroupAddress\$</i> |
| Cause | The saplgmpSnpGsrcLimitExceeded notification is generated when an IGMP source is dropped on a given SAP because a user configurable upper limit given by saplgmpSnpGCfgMaxNbrSrcs is reached. |
| Effect | The specified S,G was not added. |
| Recovery | Investigate the cause of the excessive sources. |

27.7 sdpBndIgmPsnpgGrpLimitExceeded

Table 614: 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> has exceeded the maximum limit of <i>\$sdpBndIgmPsnpgCfgMaxNbrGrps\$</i> - Dropping group <i>\$alxIgmPsnpgGroupAddress\$</i> |
| 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 615: 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 <i>\$sdpBindId\$</i> in service <i>\$svclD\$</i> has exceeded the maximum limit of <i>\$sdpBndIgmPsnpgCfgMaxNbrSrcs\$</i> - Dropping source <i>\$alxIgmPsnpgSourceAddress\$</i> for group <i>\$alxIgmPsnpgGroupAddress\$</i> |
| 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 sdpBndIgmPsnpgCfgMaxNbrGrpSrcs is reached. |
| Effect | The specified S,G was not added. |
| Recovery | Investigate the cause of the excessive sources. |

27.9 sdpBndIgmPsnpgMcacPlcyDropped

Table 616: 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 <i>\$alxIgmPsnpgGroupAddress\$</i> is dropped because of multicast CAC policy <i>\$sdpBndIgmPsnpgCfgMcacPolicyName\$</i> on SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclD\$</i> |
| 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 617: 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 <i>\$alxIgmPsnpgGroupAddress\$</i> on SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> has exceeded the maximum limit of <i>\$sdpBndIgmPsnpgCfgMaxNbrSrcs\$</i> - Dropping source <i>\$alxIgmPsnpgSourceAddress\$</i> for group <i>\$alxIgmPsnpgGroupAddress\$</i> |
| 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 618: 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 619: 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 <i>\$vRtrID\$</i> prefix <i>\$prefix\$</i> |
| 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 620: 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 <i>\$stateFrom\$</i> to <i>\$stateTo\$</i> for IP address <i>\$ip Address\$</i> sent from ethernet address <i>\$macAddress\$</i> for interface <i>\$int Name\$</i> |
| 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 621: 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 622: 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 623: 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 <i>\$macAddress\$</i> with <i>\$ipAddress\$</i> on interface <i>\$interface\$</i> |
| 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 624: 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 <i>\$ipAddress\$</i> by <i>\$macAddress\$</i> |
| Cause | ARP information has been updated. |
| Effect | None. |
| Recovery | No recovery is required. |

28.8 ipDuplicateAddress

Table 625: 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 <i>\$ipAddress\$</i> sent from ethernet address <i>\$macAddress\$</i> |
| 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 626: 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 <i>\$ipAddress\$</i> |
| 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 627: 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 <i>\$vRtrID\$</i> , prefix <i>\$prefix\$</i> , owner <i>\$routeOwner\$</i>) |
| 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 628: 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 <i>\$function\$</i> |
| 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 629: 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 <i>\$tIPsecNotifBfdIntfSvcId\$</i> interface <i>\$tIPsecNotifBfdIntfIfName\$</i> to peer <i>\$tIPsecNotifBfdIntfDestIp\$</i> changed state to <i>\$tIPsecNotifBfdIntfSessState\$</i> . |
| Cause | The operational state of a BFD session of the IPsec instance changed. |
| Effect | None. |
| Recovery | No recovery is necessary. |

29.2 tIPsecRadAcctPlcyFailure

Table 630: 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 <i>\$tIPsecRadAcctPlyName\$</i> due to: <i>\$tIPsecRadAcctPlyFailReason\$</i> |
| Cause | The tIPsecRadAcctPlyFail 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 'tIPsecRadAcctPlyFail Reason', 'tIPsecRadAcctPlyTable' configuration may need to be changed. |

29.3 tIPsecRUSAFailToAddRoute

Table 631: 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 <i>\$tIPsecRUTnlInetAddress\$</i> : <i>\$tIPsecRUTnlPort\$</i> failed to add route to <i>\$tIPsecRUSARemAddr\$</i> / <i>\$tIPsecRUSARemAPrefLen\$</i> because <i>\$tIPsecNotifReason\$</i> . |
| Cause | The event is generated when creation of a remote-user tunnel fails. |
| Effect | None. |
| Recovery | No recovery is necessary. |

29.4 tIPsecRuTnlEncapIpMtuTooSmall

Table 632: 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: <i>\$sapEncapValue\$</i> , service: <i>\$svcid\$</i> for IP address <i>\$tIPsecNotifRUTnlInetAddress\$</i> : <i>\$tIPsecNotifRUTnlPort\$</i> with configured MTU of <i>\$tIPsecNotifConfigIpMtu\$</i> , having encapsulated MTU of <i>\$tIPsecNotifConfigEncapIpMtu\$</i> has an overhead of <i>\$tIPsecNotifEncapOverhead\$</i> . |
| 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 633: tIPsecRUTnlFailToCreate properties

| Property name | Value |
|------------------|-------|
| Application name | IPSEC |

| Property name | Value |
|----------------------------------|--|
| Event ID | 2001 |
| Event name | tIPsecRUTnIFailToCreate |
| 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 <i>\$tIPsecNotifRUTnInetAddress\$</i> : <i>\$tIPsecNotifRUTnIPort\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svcid\$</i> failed because <i>\$tIPsecNotifReason\$</i> . |
| Cause | The event is generated when creation of a remote-user tunnel fails. |
| Effect | None. |
| Recovery | No recovery is necessary. |

29.6 tIPsecRUTnIRemoved

Table 634: tIPsecRUTnIRemoved properties

| Property name | Value |
|----------------------------------|---|
| Application name | IPSEC |
| Event ID | 2013 |
| Event name | tIPsecRUTnIRemoved |
| SNMP notification prefix and OID | TIMETRA-IPSEC-MIB.tmnxIPsecNotifications.13 |
| Default severity | minor |
| Source stream | main |
| Message format string | IPsec Remote-User tunnel <i>\$tIPsecNotifRUTnInetAddress\$</i> : <i>\$tIPsecNotifRUTnIPort\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svcid\$</i> was removed because <i>\$tIPsecNotifReason\$</i> . |
| Cause | A tIPsecRUTnIRemoved notification is generated when a remote-user tunnel is removed under certain reasons, which are indicated by tIPsecNotifReason (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 635: 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 | <i>\$tIPsecTrustAnchorCAProfDown\$</i> of the configured trust-anchors in profile <i>\$tIPsecTrustAnchorProfName\$</i> 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 636: 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 <i>\$tIPsecNotifIPsecTunnelName\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svcid\$</i> with configured MTU of <i>\$tIPsecNotifConfigIpMtu\$</i> , having encapsulated MTU of <i>\$tIPsecNotifConfigEncapIpMtu\$</i> has an overhead of <i>\$tIPsecNotifEncapOverhead\$</i> |
| 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 637: 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 <i>\$tIPsecNotifTunnelIdentifier\$</i> of type <i>\$tIPsecNotifTunnelType\$</i> had an abnormal protocol event due to <i>\$tIPsecNotifReason\$</i> . |

| 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 638: 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 <i>\$tmnxIPsecGWName</i> \$ on service <i>\$svcid</i> and SAP <i>\$sapEncapValue</i> , admin state: <i>\$tmnxIPsecGWAdminState</i> , oper state: <i>\$tmnxIPsecGWOperState</i> , oper flags: <i>\$tmnxIPsecGWOperFlags</i> |
| 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 <code>tmnxIPsecGWOperFlags</code> for information on why the gateway is operationally down. |

29.11 `tmnxIPsecTunnelOperStateChange`

Table 639: `tmnxIPsecTunnelOperStateChange` properties

| Property name | Value |
|----------------------------------|--|
| Application name | IPSEC |
| Event ID | 2011 |
| Event name | <code>tmnxIPsecTunnelOperStateChange</code> |
| SNMP notification prefix and OID | TIMETRA-IPSEC-MIB. <code>tmnxIPsecNotifications.11</code> |
| Default severity | minor |
| Source stream | main |
| Message format string | Operational state change for IPsec Tunnel <code>\$tmnxIPsecTunnelName\$</code> on service <code>\$svclD\$</code> and SAP <code>\$sapEncapValue\$</code> , admin state: <code>\$tmnxIPsecTunnelAdminState\$</code> , oper state: <code>\$tmnxIPsecTunnelOperState\$</code> , oper flags: <code>\$tmnxIPsecTunnelOperFlags\$</code> |
| Cause | The <code>tmnxIPsecTunnelOperStateChange</code> notification is generated when there is a change in <code>tmnxIPsecTunnelOperState</code> for an IPsec tunnel. |
| Effect | When the value of <code>tmnxIPsecTunnelOperState</code> 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 <code>tmnxIPsecTunnelOperState</code> is 'inService (2)', the IPsec tunnel is operationally up. When the value of <code>tmnxIPsecGWOperState</code> 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 <code>tmnxIPsecTunnelOperFlags</code> are cleared. |
| Recovery | Please refer to <code>tmnxIPsecTunnelOperFlags</code> for information on why the tunnel is operationally down. |

29.12 `tmnxSecNotifCmptedCertChnChngd`

Table 640: *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 <i>\$tIPsecNotifCaProfNames\$</i> in cert-profile <i>\$tIPsecNotifCertProfileName\$</i> entry <i>\$tIPsecNotifCertProfEntryId\$</i> |
| 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 641: *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 <i>\$tIPsecNotifCertProfileName\$</i> entry <i>\$tIPsecNotifCertProfEntryId\$</i> due to CA profile <i>\$tIPsecNotifCaProfNames\$</i> |
| Cause | The <i>tmnxSecNotifCmptdCertHashChngd</i> 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 642: *tmnxSecNotifSendChnNotInCmptChn* properties

| Property name | Value |
|----------------------------------|---|
| Application name | IPSEC |
| Event ID | 2010 |
| Event name | <i>tmnxSecNotifSendChnNotInCmptChn</i> |
| SNMP notification prefix and OID | TIMETRA-IPSEC-MIB. <i>tmnxIPsecNotifications.10</i> |
| Default severity | minor |
| Source stream | security |
| Message format string | Send-chain CA profile <i>\$tIPsecNotifCaProfNames\$</i> not in the computed certificate chain of cert-profile <i>\$tIPsecNotifCertProfileName\$</i> entry <i>\$tIPsecNotifCertProfEntryId\$</i> |
| Cause | The <i>tmnxSecNotifSendChnNotInCmptChn</i> 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 643: 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 <i>\$isisSAdjState\$</i> for interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , LSP-id: <i>\$vRtrIsisTrapLSPIDString\$</i> |
| 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 isisSAdjState is the new state of the adjacency. |
| Effect | No effect. |
| Recovery | No recovery is necessary. |

30.2 tmnxIsisAdjBfdSessionSetupFail

Table 644: 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 <i>\$tmnxIsisBfdSessSetupFail Reason\$</i> for interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystem Level\$</i> , LSP-id: <i>\$tmnxIsisNotifTrapLSPIDString\$</i> |
| 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 645: 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 <i>\$tmnxIsisISAdjRestart Status\$</i> for interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystem Level\$</i> |
| 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 646: 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: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , fragment: <i>\$vRtrIsisPDUFragmentString\$</i> , LSP size: <i>\$tmnxIsisNotifLSPSize\$</i> |
| 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 647: *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: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , fragment: <i>\$vRtrIsisPDUFragmentString\$</i> |
| Cause | The <i>tmnxIsisAuthFail</i> 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 648: *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: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , fragment: <i>\$vRtrIsisPDUFragmentString\$</i> |
| Cause | The <i>tmnxIsisAutTypeFail</i> 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 tmnxIsisCirclDExhausted

Table 649: *tmnxIsisCirclDExhausted* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2046 |
| Event name | <i>tmnxIsisCirclDExhausted</i> |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB. <i>tmnxIsisNotifications.18</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Circuit-id space exhausted for level <i>\$tmnxIsisNotifSystemLevel\$</i> - interface: <i>\$vRtrIfIndex\$</i> |
| Cause | The <i>tmnxIsisCirclDExhausted</i> 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 650: 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: <i>\$vRtrIfIndex\$</i> (level <i>\$tmnxIsisNotifSystemLevel\$</i>): <i>\$tmnxIsisNotifCircMtuSize\$</i> smaller than <i>\$tmnxIsisNotifCircMinReqMtuSize\$</i> (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 651: 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: <i>\$vRtrIfIndex\$</i> , level: <i>\$tmnxIsisNotifSystemLevel\$</i> , with LSP-id: <i>\$vRtrIsisTrapLSPIDString\$</i> . |
| Cause | The tmnxIsisCorruptedLSPDetected notification is generated when we find that an 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 652: 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 <i>\$tmnxIsisLSPLifetimeRemain\$</i> received on LSP <i>\$tmnxIsisLSPIdString\$</i> , for level: <i>\$tmnxIsisLevel\$</i> |
| 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 <code>tmnxIsisMinRemainingLspLifetime</code> value. |

30.11 tmnxIsisDatabaseOverload

Table 653: *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 <i>\$tmnxIsisLevelOverloadStatus\$</i> , system level: <i>\$tmnxIsisNotifSystemLevel\$</i>) - Level1State: <i>\$isisSysL1State\$</i> , Level2State: <i>\$isisSysL2State\$</i> <i>\$tmnxIsisNotifyDescription\$</i> |
| Cause | The <code>tmnxIsisDatabaseOverload</code> notification is generated when the system enters or leaves the Overload state. |
| Effect | Database is overloaded. |
| Recovery | No recovery is necessary unless <code>tmnxIsisNotifyDescription</code> indicates it. |

30.12 tmnxIsisExportLimitReached

Table 654: *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 <i>\$tmnxIsisNotifSystemLevel\$</i> has reached the export-limit <i>\$tmnxIsisExportLimit\$</i> , 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 655: *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 <i>\$tmnxIsisNotifSystemLevel\$</i> has reached <i>\$tmnxIsisExportLimitLogPercent\$</i> percent of the export limit <i>\$tmnxIsisExportLimit\$</i> |

| 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, tmnxIsisExportLimit. 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 656: 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 : <i>\$tmnxIsisFailureReasonCode\$</i> |
| Cause | A tmnxIsisFailureDisabled notification is generated when ISIS is operationally brought down. Reason for the failure is indicated by tmnxIsisFailureReasonCode. |
| Effect | ISIS is now operationally down. |
| Recovery | ISIS will auto restart. |

30.15 tmnxIsisFaOperParticipationDown

Table 657: *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 <i>\$tmnxIsisFlexAlgoId\$</i> in level <i>\$tmnxIsisNotifSystemLevel\$</i> is operationally down due to <i>\$tmnxIsisNotifyDescription\$</i> . |
| 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 658: *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: <i>\$tmnxIsisNotifFieldLen\$</i> , interface: <i>\$vRtrIfIndex\$</i> , on fragment: <i>\$vRtrIsisPDUFragmentString\$</i> |
| 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 659: 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 <i>\$vRtrIfIndex\$</i> because Exit State <i>\$tmnxIsisIfLdpSyncTimerState\$</i> |
| 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 vRtrIfLdpSyncTimer. |

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

30.18 tmnxIisisLdpSyncTimerStarted

Table 660: tmnxIisisLdpSyncTimerStarted properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2048 |
| Event name | tmnxIisisLdpSyncTimerStarted |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIisisNotifications.20 |
| Default severity | warning |
| Source stream | main |
| Message format string | IGP-LDP synchronization timer has started for interface \$vRtrIfIndex\$. |
| Cause | The tmnxIisisLdpSyncTimerStarted 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 tmnxIisisLSPPurge

Table 661: tmnxIisisLSPPurge properties

| Property name | Value |
|------------------|-------------------|
| Application name | ISIS |
| Event ID | 2060 |
| Event name | tmnxIisisLSPPurge |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.32 |
| Default severity | warning |
| Source stream | main |
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> LSP Purge - interface: <i>\$vRtrIfIndex\$</i>, on level: <i>\$tmnxIsisNotifSystemLevel\$</i>, LSP: <i>\$vRtrIsisTrapLSPIDString\$</i>, POI SysId: <i>\$tmnxIsisNotifPurgeOriginatorString\$</i> - <i>\$tmnxIsisNotifAdditionalInfo\$</i> LSP Purge - interface: <i>\$vRtrIfIndex\$</i>, on level: <i>\$tmnxIsisNotifSystemLevel\$</i>, LSP: <i>\$vRtrIsisTrapLSPIDString\$</i>, POI sysId: <i>\$tmnxIsisNotifPurgeOriginatorString\$</i>, rcvd sysId: <i>\$tmnxIsisNotifPurgeSourceString\$</i> - <i>\$tmnxIsisNotifAdditionalInfo\$</i> |
| 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 662: 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: <i>\$tmnxIsisNotifLSPSize\$</i> , on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , LSP-id: <i>\$vRtrIsisTrapLSPIDString\$</i> |

| 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 663: 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 <i>\$isisManAreaAddrString\$</i> 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 <i>isisManAreaAddrExistState</i> 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 664: *tmnxIisisMaxAreaAddrsMismatch* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2034 |
| Event name | tmnxIisisMaxAreaAddrsMismatch |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIisisNotifications.6 |
| Default severity | warning |
| Source stream | main |
| Message format string | Max area addresses mismatch - max area addresses: <i>\$tmnxIisisNotifMaxAreaAddress\$</i> , interface: <i>\$vRtrIfIndex\$</i> , on fragment: <i>\$vRtrIisisPDUFragmentString\$</i> |
| Cause | The <i>tmnxIisisMaxAreaAddrsMismatch</i> 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 *tmnxIisisMaxSeqExceedAttempt*

Table 665: *tmnxIisisMaxSeqExceedAttempt* properties

| Property name | Value |
|----------------------------------|--|
| Application name | ISIS |
| Event ID | 2032 |
| Event name | tmnxIisisMaxSeqExceedAttempt |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIisisNotifications.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: <i>\$tmnxIsisNotifSystemLevel\$</i> , with LSP-id: <i>\$vRtrIsisTrapLSPIDString\$</i> . Shutdown for a while and start over. |
| Cause | The <i>tmnxIsisMaxSeqExceedAttempt</i> 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 666: *tmnxIsisOrigLSPBufSizeMismatch* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2043 |
| Event name | <i>tmnxIsisOrigLSPBufSizeMismatch</i> |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB. <i>tmnxIsisNotifications.15</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Originating LSP buffer size mismatch - LSP size: <i>\$tmnxIsisNotifOriginatingBuffSize\$</i> , on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , LSP-id: <i>\$vRtrIsisTrapLSPIDString\$</i> |
| Cause | The <i>tmnxIsisOrigLSPBufSizeMismatch</i> notification is sent when a Level 1 LSP or Level 2 LSP is received which is larger than the local value for <i>isisSysOrigL1LSPBuffSize</i> or <i>isisSysOrigL2LSPBuffSize</i> respectively, or when a Level 1 LSP or Level2 LSP is received containing the <i>originatingLSPBufferSize</i> option and the value in the PDU option field does not match the local value for <i>isisSysOrigL1LSPBuffSize</i> or <i>isisSysOrigL2LSPBuffSize</i> 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 667: 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: <i>\$vRtrIfIndex\$</i> , on level: <i>\$tmnxIsisNotifSystemLevel\$</i> , LSP: <i>\$vRtrIsisTrapLSPIDString\$</i> |
| 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 668: *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 <i>\$tmnxIsisNotifAdditionalInfo\$</i> |
| Cause | The <i>tmnxIsisPfxLimitOverloadWarning</i> notification is sent when the number of prefixes in the system reaches the <i>tmnxIsisPrefixLimit</i> Threshold or the <i>tmnxIsisPrefixLimit</i> . |
| Effect | When <i>tmnxIsisPrefixLimit</i> is not yet reached, but the <i>tmnxIsisPrefixLimit</i> Threshold is reached there is no direct effect; but when the number of prefixes grows the system might go into overload. When the <i>tmnxIsisPrefixLimit</i> is reached and the object <i>tmnxIsisPrefixLimitLogOnly</i> is false, IS-IS will be into overload. There is no direct effect when the object <i>tmnxIsisPrefixLimitLogOnly</i> is true. |
| Recovery | Increase the IS-IS prefix limit. |

30.27 tmnxIsisProtoSuppMismatch

Table 669: *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: <i>\$tmnxIsisNotif ProtocolsSupported\$</i> , on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , LSP-id: <i>\$vRtrIsisTrapLSPIDString\$</i> |
| Cause | The <i>tmnxIsisProtoSuppMismatch</i> 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 670: *tmnxIsisRejectedAdjacency* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2041 |
| Event name | <i>tmnxIsisRejectedAdjacency</i> |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB. <i>tmnxIsisNotifications.13</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Rejected adjacency on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> |
| Cause | The <i>tmnxIsisRejectedAdjacency</i> 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 671: 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: <i>\$tmnxIsisNotifyIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , description: <i>\$tmnxIsisNotifyDescription\$</i> |
| 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 672: 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: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIisisNotifSystemLevel\$</i> , description: <i>\$tmnxIisisNotifyDescription\$</i> |
| Cause | The <i>tmnxIisisRejectedAdjacencySid</i> 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 *tmnxIisisRejectedEndXSid*

Table 673: *tmnxIisisRejectedEndXSid* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2069 |
| Event name | <i>tmnxIisisRejectedEndXSid</i> |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB. <i>tmnxIisisNotifications.41</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Failed end-x SID on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIisisNotifSystemLevel\$</i> , description: <i>\$tmnxIisisNotifyDescription\$</i> |
| Cause | The <i>tmnxIisisRejectedEndXSid</i> 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 tmnxIsisRejectedPgld

Table 674: tmnxIsisRejectedPgld properties

| Property name | Value |
|----------------------------------|--|
| Application name | ISIS |
| Event ID | 2070 |
| Event name | tmnxIsisRejectedPgld |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIsisNotifications.42 |
| Default severity | warning |
| Source stream | main |
| Message format string | Failed PGID on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , description: <i>\$tmnxIsisNotifyDescription\$</i> |
| Cause | The tmnxIsisRejectedPgld 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 675: 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 <i>\$tmnxIsisNotifSystemLevel\$</i> has dropped below the export limit <i>\$tmnxIsisExportLimit\$</i> |
| 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 676: *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: <i>\$vRtrIsisTrapLSPIDString\$</i> , on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> |
| 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 tmnxIisisSidError

Table 677: tmnxIisisSidError properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2057 |
| Event name | tmnxIisisSidError |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIisisNotifications.29 |
| Default severity | minor |
| Source stream | main |
| Message format string | <i>\$tmnxIisisNotifyDescription\$</i> SID: <i>\$tmnxIisisPrefixSidValue\$</i> , level: <i>\$tmnxIisisPrefixSidLevel\$</i> , mtid: <i>\$tmnxIisisRouteMtlId\$</i> , type: <i>\$tmnxIisisPrefixSidType\$</i> , flags: <i>\$tmnxIisisPrefixSidFlags\$</i> , algo: <i>\$tmnxIisisPrefixSidAlgorithm\$</i> |
| 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 tmnxIisisSidNotInLabelRange

Table 678: *tmnxIisisSidNotInLabelRange* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2058 |
| Event name | tmnxIisisSidNotInLabelRange |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIisisNotifications.30 |
| Default severity | minor |
| Source stream | main |
| Message format string | SID not in range of router: <i>\$tmnxIisisNotifPfxSidSysIDString\$</i> , SID: <i>\$tmnxIisisPrefixSidValue\$</i> , startLabel: <i>\$tmnxIisisNotifPfxSidRangeStartLbl\$</i> , maxIdx: <i>\$tmnxIisisNotifPfxSidRangeMaxIdx\$</i> level: <i>\$tmnxIisisPrefixSidLevel\$</i> , mtid: <i>\$tmnxIisisRouteMtid\$</i> , type: <i>\$tmnxIisisPrefixSidType\$</i> , flags: <i>\$tmnxIisisPrefixSidFlags\$</i> , algo: <i>\$tmnxIisisPrefixSidAlgorithm\$</i> |
| 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 tmnxIisisSidStatsIndexAlloc

Table 679: *tmnxIisisSidStatsIndexAlloc* properties

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

| Property name | Value |
|-----------------------|--|
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> Statistics Index Allocation status changed to <i>\$tmnxIisisNotifStats IndexStatus\$</i> for adjacency-set <i>\$tmnxIisisSidStatsAdjSet\$</i> Statistics Index Allocation status changed to <i>\$tmnxIisisNotifStats IndexStatus\$</i> for adjacency interface <i>\$tmnxIisisSidStatsIfIndex\$</i> Statistics Index Allocation status changed to <i>\$tmnxIisisNotifStats IndexStatus\$</i> for node <i>\$tmnxIisisSidStatsPrefix\$/\$tmnxIisisSidStats PrefixLength\$</i> |
| Cause | The <i>tmnxIisisSidStatsIndexAlloc</i> 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 tmnxIisisSrgbBadLabelRange

Table 680: *tmnxIisisSrgbBadLabelRange* properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2063 |
| Event name | <i>tmnxIisisSrgbBadLabelRange</i> |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB. <i>tmnxIisisNotifications.35</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Bad SRGB label range for advertising router: <i>\$tmnxIisisNotifSrgbAdv RtrSysIDString\$</i> , startLabel: <i>\$tmnxIisisNotifSrgbRangeStartLbl\$</i> , maxIdx: <i>\$tmnxIisisNotifSrgbRangeMaxIdx\$</i> , level: <i>\$tmnxIisisNotifSrgbLevel\$</i> , mtid: <i>\$tmnxIisisNotifSrgbMtlD\$ \$tmnxIisisNotifAdditionalInfo\$</i> |
| Cause | The <i>tmnxIisisSrgbBadLabelRange</i> 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 tmnxIisisSrv6LocError

Table 681: tmnxIisisSrv6LocError properties

| Property name | Value |
|----------------------------------|--|
| Application name | ISIS |
| Event ID | 2071 |
| Event name | tmnxIisisSrv6LocError |
| SNMP notification prefix and OID | TIMETRA-ISIS-NG-MIB.tmnxIisisNotifications.43 |
| Default severity | warning |
| Source stream | main |
| Message format string | <i>\$tmnxIisisNotifyDescription\$, level:\$tmnxIisisNotifSystemLevel\$, mtid:\$tmnxIisisRouteMtlId\$, algo:\$tmnxIisisSrv6SidAlgorithm\$</i> |
| 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 tmnxIisisSrv6StaticSidIfTypeError

Table 682: *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 | <p>Possible messages:</p> <ul style="list-style-type: none"> Unable to install static SID <i>\$tmnxIsisSrv6SidValue\$</i> with behavior <i>\$tmnxIsisSrv6SidEndpointBehavior\$</i> on interface <i>\$vRtrIfIndex\$</i> of type <i>\$tmnxIsisIfOperType\$</i>, description: <i>\$tmnxIsisNotifyDescription\$</i> Unable to install static USID <i>\$tmnxIsisSrv6USidValue\$</i> with behavior <i>\$tmnxIsisSrv6USidEndpointBehavior\$</i> on interface <i>\$vRtrIfIndex\$</i> of type <i>\$tmnxIsisIfOperType\$</i>, description: <i>\$tmnxIsisNotifyDescription\$</i> |
| 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 bcst; or when a new ISIS bcst 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 683: *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 - <i>\$tmnxIsisNotifProtocolVersion\$</i> on interface: <i>\$vRtrIfIndex\$</i> , for level: <i>\$tmnxIsisNotifSystemLevel\$</i> , fragment: <i>\$vRtrIsisPDUFragmentString\$</i> |
| 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 684: 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 <i>\$vRtrIsisNbrSysIdString\$</i> on interface <i>\$vRtrIfIndex\$</i> at system level <i>\$vRtrIsisSystemLevel\$</i> |
| 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 vRtrIisisSpbNbrMultAdjExistsClear

Table 685: vRtrIisisSpbNbrMultAdjExistsClear properties

| Property name | Value |
|----------------------------------|---|
| Application name | ISIS |
| Event ID | 2026 |
| Event name | vRtrIisisSpbNbrMultAdjExistsClear |
| SNMP notification prefix and OID | TIMETRA-ISIS-MIB.vRtrIisisNotifications.26 |
| Default severity | warning |
| Source stream | main |
| Message format string | SPB multiple adjacency cleared for neighbor <i>\$vRtrIisisNbrSysIdString\$</i> on interface <i>\$vRtrIifIndex\$</i> at system level <i>\$vRtrIisisSystemLevel\$</i> |
| Cause | A vRtrIisisSpbNbrMultAdjExistsClear notification is sent when an IS-IS SPB instance clears the condition raised by vRtrIisisSpbNbrMultAdjExists 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 686: 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.vRtrIisisNotifications.27 |
| Default severity | warning |
| Source stream | main |
| Message format string | SPB ect-algorithm changed to <i>\$vRtrSpbEctFidAlgorithm\$</i> for FID range <i>\$vRtrSpbEctFidStart\$-\$vRtrSpbEctFidEnd\$</i> under <i>\$vRtrIisisLevel\$</i> |
| 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 687: *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 - <i>\$tmnxL2tpNotifyDescription\$</i> . |
| 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 tmnxL2tplsaMdaVRtrStateChange

Table 688: *tmnxL2tplsaMdaVRtrStateChange* properties

| Property name | Value |
|------------------|-------------------------------|
| Application name | L2TP |
| Event ID | 2002 |
| Event name | tmnxL2tplsaMdaVRtrStateChange |

| 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 <i>\$tmnxL2tpIsaMdaVRtrOperState\$</i> . <i>\$tmnxL2tpNotifyDescription\$</i> . |
| 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 689: *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 <i>\$tmnxL2tpPppNcpFailureProtocol\$</i> phase failure for user <i>\$tmnxL2tpLnsSePppPppUserName\$</i> interface <i>\$vRtrIfName\$</i> service <i>\$tmnxL2tpLnsSePppSvcId\$</i> - <i>\$tmnxL2tpNotifyDescription\$</i> |
| Cause | The tmnxL2tpLnsPppNcpFailure notification indicates that there is an NCP phase setup problem. |
| Effect | N/A |
| Recovery | N/A |

31.4 tmnxL2tpLnsSePppSessionFailure

Table 690: 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: <ul style="list-style-type: none"> L2TP session \$vRtrID\$: \$tmnxL2tpSeStatusId\$, user \$tmnxL2tpLnsSePppPppUserName\$ - \$tmnxL2tpNotifyDescription\$ L2TP session \$vRtrID\$: \$tmnxL2tpSeStatusId\$, user \$tmnxL2tpLnsSePppPppUserName\$ (interface \$tmnxL2tpLnsSePppGrplf\$, 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 691: 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 <i>\$tmnxL2tpTuStatusPeerAddr\$</i> (port <i>\$tmnxL2tpTuStatusRemoteUdpPort\$</i>) changed to <i>\$tmnxL2tpPeerStatUnreachable\$. \$tmnxL2tpNotifyDescription\$</i> . |
| Cause | The <i>tmnxL2tpPeerUnreachable</i> notification is generated when the peer becomes unreachable, and then becomes reachable again. The cause may be specified in the <i>tmnxL2tpNotifyDescription</i> . |
| Effect | N/A |
| Recovery | N/A |

31.6 tmnxL2tpTunnelBlacklisted

Table 692: *tmnxL2tpTunnelBlacklisted* properties

| Property name | Value |
|----------------------------------|---|
| Application name | L2TP |
| Event ID | 2006 |
| Event name | <i>tmnxL2tpTunnelBlacklisted</i> |
| SNMP notification prefix and OID | TIMETRA-L2TP-MIB. <i>tmnxL2tpNotifications.12</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | The unreachability of L2TP tunnel <i>\$tmnxL2tpTuStatusId</i> in vRtr <i>\$vRtrId</i> changed to <i>\$tmnxL2tpTuStatusSelBlacklstState. \$tmnxL2tpNotifyDescription\$</i> . |
| Cause | The <i>tmnxL2tpTunnelBlacklisted</i> 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 693: *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 \$tmnxL2tpStatCurrSelBlacklistLen 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 694: *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 <i>\$tmnxL2tpVappVRtrOperState\$</i> . <i>\$tmnxL2tpNotifyDescription\$</i> . |
| Cause | The <i>tmnxL2tpVappVRtrStateChange</i> 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 695: 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 <i>\$tLagIndex\$</i> 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 696: 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 <i>\$tLagIndex\$</i> 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 697: 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 <i>\$tmnxPortPortID\$</i> to LAG <i>\$tLagIndex\$</i> because <i>\$tLagNotifyPortAddFailReason\$</i> |
| 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 698: 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 <i>\$tmnxPortPortID\$</i> to LAG <i>\$tLagIndex\$</i> is resolved - <i>\$tLagNotifyPortAddFailReason\$</i> |
| Cause | The failure reported by notification tLagPortAddFailed has been resolved. |
| Effect | N/A |
| Recovery | N/A |

32.5 LagStateEvent

Table 699: 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 <i>\$tLagIndex\$</i> : <i>\$tLagNotifyAdditionalInfo\$</i> |

| 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 700: 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 | <i>\$tLagNotifySubGroupSelected\$</i> |
| 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 701: 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 <i>\$tLagIndex\$</i> adaptive load balancing changed - <i>\$tLagNotifyAdditionalInfo\$</i> |
| 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 702: 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 <i>\$tLagIndex\$</i> : <i>\$tLagNotifyAdditionalInfo\$</i> |
| 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 703: *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 <i>\$tLagIndex\$</i> member <i>\$tmnxPortPortID\$</i> BFD state changed to <i>\$tmnxLagBfdMemState\$</i> - <i>\$tLagNotifyAdditionalInfo\$</i> |
| 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 704: 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 <i>\$tmnxLdapOperState\$</i> |
| Cause | [CAUSE]The tmnxLdapOperStateChange notification is generated when the tmnxLdapOperState has transitioned either from 'outOfService' 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 tmnxLdapOperState 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 705: *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 ' <i>\$tmnxLdapServerName\$</i> ' (ID: <i>\$tmnxLdapServerIndex\$</i>) (<i>\$tmnxLdapServerInetAddress\$:\$tmnxLdapServerPort\$</i>) has changed to <i>\$tmnxLdapServerOperState\$</i> |
| Cause | [CAUSE]The <i>tmnxLdapServerOperStateChange</i> notification is generated when the <i>tmnxLdapServerOperState</i> has transitioned either from 'outOfService' to 'inService' or from 'inService' to 'outOfService' state. [EFFECT]If <i>tmnxLdapServerOperState</i> has transitioned to 'outOfService' state then the particular LDAP server connection is not available for use. If <i>tmnxLdapServerOperState</i> has transitioned to 'inService' state then the particular LDAP server is available for use. [RECOVERY]If the new state corresponds to the <i>tmnxLdapServerAdminState</i> , then this is the desirable behavior and no recovery is needed. If the new state of the <i>tmnxLdapServerOperState</i> object is 'outOfService' while the value of the object <i>tmnxLdapServerAdminState</i> 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 706: 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: <i>\$vRtrLdpNotifyLocalGroupID\$</i> , remote group ID: <i>\$vRtrLdpNotifyRemoteGroupID\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

34.2 vRtrLdpNgAddrFecCommMismatch

Table 707: 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: <i>\$vRtrID\$</i> Community vRtrLdpNgAddrFecCommunity |
| 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 708: 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: <i>\$vRtrID\$</i> , <i>\$interfaceName\$</i> , administrative state: <i>\$vRtrLdpNgIfAdminState\$</i> , operational state: <i>\$vRtrLdpNgIfOperState\$</i> |

| 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 709: vRtrLdpNgInetIfStateChange properties

| Property name | Value |
|----------------------------------|---|
| Application name | LDP |
| Event ID | 2014 |
| Event name | vRtrLdpNgInetIfStateChange |
| SNMP notification prefix and OID | TIMETRA-LDP-NG-MIB.tmxLdpNgNotifications.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 710: 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: \$vRtrLdpNgGenIpv4OperState\$, reason: \$vRtrLdpNgGenIpv4OperDownReason\$ |
| Cause | The vRtrLdpNgIpv4InstStateChange is generated when the IPv4 LDP instance changes state operationally as specified by vRtrLdpNgGenIpv4OperState. |
| 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 711: 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: <i>\$vRtrID\$</i> , administrative state: <i>\$vRtrLdpNgGenAdminState\$</i> , operational state: <i>\$vRtrLdpNgGenIPv6OperState\$</i> , reason: <i>\$vRtrLdpNgGenIPv6OperDownReason\$</i> |
| Cause | The vRtrLdpNgIpv6InstStateChange is generated when the IPv6 LDP instance changes state operationally as specified by vRtrLdpNgGenIPv6OperState. |
| 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 712: 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: <i>\$vRtrID\$</i> |
| 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 713: 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 <i>\$vRtrLdpNgSessState\$</i> . Overload Notification message is <i>\$vRtrLdpNgSessOverloadDirection\$</i> to/from peer <i>\$vRtrLdpNgPeerLdpId\$</i> with overload state <i>\$vRtrLdpNgSessOverloadState\$</i> for fec type <i>\$vRtrLdpNgSessOverloadFecType\$</i> and sub type fec <i>\$vRtrLdpNgSessOvldFecTypeSubTyp\$</i> |
| 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 vRtrLdpNgSessOverloadFecType and vRtrLdpNgSessOvldFecTypeSubTyp, then appropriate LDP configuration changes may be required on the Local and/or Remote LSR. Once the Local LSR is not overloaded anymore, an LDP Overload Notification message is sent to the peer vRtrLdpNgPeerLdpId and vRtrLdpNgSessOverloadState has the value of 'false' for given fec and sub type fec. |

34.9 vRtrLdpNgSessMaxFecLimitReached

Table 714: 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 <i>\$vRtrLdpNgPeerAddress\$</i> has reached the maximum value of <i>\$vRtrLdpNgSessParamMaxFec\$</i> . The current operational threshold is <i>\$vRtrLdpNgSessOperMaxFecThreshold\$</i> 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 vRtrLdpNgSessMaxFecLimitReached 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 (vRtrLdpNgSessParamMaxFec) it results in any of the following: (1) If vRtrLdpNgSessParamMaxFecLogOnly 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 vRtrLdpNgSessParamMaxFecLogOnly 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 715: 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 <i>\$vRtrLdpNgPeerAddress\$</i> has gone <i>\$vRtrLdpNgSessOperThresLevel\$</i> the configured threshold of the maximum value <i>\$vRtrLdpNgSessParamMaxFec\$</i> . The current operational threshold is <i>\$vRtrLdpNgSessOperMaxFecThreshold\$</i> 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 716: 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 717: 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 <i>\$vRtrLdpStatus\$d</i> |
| 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 718: 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 <i>\$srcAddr\$</i> : <i>\$prompt\$ \$message\$</i> |
| 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 719: 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 <i>\$srcAddr\$</i> . <i>\$message\$</i> : <i>\$prompt\$ \$command\$</i> |
| 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 720: 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 <i>\$srcAddr\$</i> . <i>\$message\$</i> : <i>\$prompt\$ \$command\$</i> |
| 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 721: 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 722: 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 723: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 724: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> min |
| Cause | A <i>tmnxUserCliLoginMaxAttempts</i> 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 <i>tmnxPasswordAttemptsTime</i> minutes. The value of the object <i>tmnxPasswordAttemptsCount</i> indicates the maximum number of unsuccessful login attempts allowed. The value of the object <i>tmnxPasswordAttemptsLockoutPeriod</i> 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 <i>tmnxSecNotifyUserName</i> indicates the name of the user attempting to open a CLI session. The value of the object <i>tmnxSecNotifyAddrType</i> indicates the type of the IP address stored in the object <i>tmnxSecNotifyAddr</i> . The value of the object <i>tmnxSecNotifyAddr</i> indicates the IP address of the user attempting to open a CLI session. |
| Effect | The user is locked out for a period of <i>tmnxPasswordAttemptsLockoutPeriod</i> minutes. A remote access session is terminated. |
| Recovery | No recovery action is required. |

35.8 cli_user_logout

Table 725: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 726: 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 <i>\$tMirrorDestinationIndex\$</i> 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 727: 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 <i>\$tMirrorDestinationIndex\$</i> 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 728: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 729: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 730: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> 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 <code>tmnxPasswordAttemptsTime</code> minutes. The value of the object <code>tmnxPasswordAttemptsCount</code> indicates the maximum number of unsuccessful login attempts allowed. The value of the object <code>tmnxPasswordAttemptsLockoutPeriod</code> 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 <code>tmnxSecNotifyUserName</code> indicates the name of the user attempting to connect via FTP. The value of the object <code>tmnxSecNotifyAddrType</code> indicates the type of the IP address stored in the object <code>tmnxSecNotifyAddr</code> . The value of the object <code>tmnxSecNotifyAddr</code> indicates the IP address of the user attempting to connect via FTP. |
| Effect | The user is locked out for a period of <code>tmnxPasswordAttemptsLockoutPeriod</code> minutes. An FTP session is terminated. |
| Recovery | No recovery action is required. |

35.14 ftp_user_logout

Table 731: 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 <code>\$userName\$</code> from <code>\$srcAddr\$</code> logged out |
| Cause | A user logged out. |
| Effect | The user access session ends. |
| Recovery | No recovery is required |

35.15 grpc_auth

Table 732: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 733: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 734: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 735: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 736: *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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> 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 <i>tmnxPasswordAttemptsTime</i> minutes. The value of the object <i>tmnxPasswordAttemptsCount</i> indicates the maximum number of unsuccessful login attempts allowed. The value of the object <i>tmnxPasswordAttemptsLockoutPeriod</i> 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 <i>tmnxSecNotifyUserName</i> 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 737: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | The user access session ends. |
| Recovery | No recovery is required |

35.21 host_snmp_attempts

Table 738: *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 <i>\$hostAddress\$</i> is locked out for <i>\$lockoutTime\$</i> 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 739: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> [session ID <i>\$sessionId\$</i>]: <i>\$prompt\$ \$command\$</i> |
| 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 740: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> [session ID <i>\$sessionId\$</i>]. Command not allowed for this user: <i>\$prompt\$ \$command\$</i> |
| 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 741: 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 <i>\$userName\$</i> (<i>\$interface\$</i>) from <i>\$srcAddr\$</i> 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 742: 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 743: 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: <i>\$fileName\$</i> |
| 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 744: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 745: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 746: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 747: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 748: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> min |
| Cause | A <i>tmnxUserNetconfLoginMaxAttempts</i> 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 <i>tmnxPasswordAttemptsTime</i> minutes. The value of the object <i>tmnxPasswordAttemptsCount</i> indicates the maximum number of unsuccessful login attempts allowed. The value of the object <i>tmnxPasswordAttemptsLockoutPeriod</i> 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 <i>tmnxSecNotifyUserName</i> indicates the name of the user attempting to open a netconf session. The value of the object <i>tmnxSecNotifyAddrType</i> indicates the type of the IP address stored in the object <i>tmnxSecNotifyAddr</i> . The value of the object <i>tmnxSecNotifyAddr</i> indicates the IP address of the user attempting to open a netconf session. |
| Effect | The user is locked out for a period of <i>tmnxPasswordAttemptsLockoutPeriod</i> minutes. A remote access session is terminated. |
| Recovery | No recovery action is required. |

35.32 netconf_user_logout

Table 749: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | A user access session ended. |
| Recovery | No recovery is required |

35.33 radiusFailed

Table 750: 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: <i>\$tMirrorNotifyLiDescription\$</i> |
| 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 751: *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: <i>\$sliConfigStatus\$</i> . LI separate: <i>\$sbiLiSeparate\$</i> . LI local save: <i>\$sbiLiLocalSave\$</i> . System last booted time: <i>\$sysUpTime\$</i> . |
| 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 752: *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: <i>\$fileName\$</i> |
| 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 753: *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 <i>\$srcAddr\$</i> > <i>\$vbList\$</i> |
| 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 754: *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 <i>\$tMirrorSourceIndex\$</i> 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 755: 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 <i>\$tMirrorSourceIndex\$</i> 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 756: 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 <i>\$tMirrorSourceIndex\$</i> associated SAP <i>\$tMirrorSourceSapEncapValue\$</i> has been <i>\$tMirrorSourceChangeType\$</i> |
| 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 757: 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 <i>\$tMirrorSourceIndex\$</i> subscriber " <i>\$tMirrorSourceSubIdent\$</i> " has been <i>\$tMirrorSourceChangeType\$</i> |
| 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 758: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 759: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 760: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> min |
| Cause | A <i>tmnxLiUserSshLoginMaxAttempts</i> 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 <i>tmnxPasswordAttemptsTime</i> minutes. The value of the object <i>tmnxPasswordAttemptsCount</i> indicates the maximum number of unsuccessful login attempts allowed. The value of the object <i>tmnxPasswordAttemptsLockoutPeriod</i> 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 <i>tmnxSecNotifyUserName</i> indicates the name of the user attempting to connect via SSH. The value of the object <i>tmnxSecNotifyAddrType</i> indicates the type of the IP address stored in the object <i>tmnxSecNotifyAddr</i> . The value of the object <i>tmnxSecNotifyAddr</i> indicates the IP address of the user attempting to connect via SSH. |
| Effect | The user is locked out for a period of <i>tmnxPasswordAttemptsLockoutPeriod</i> minutes. An SSH session is terminated. |
| Recovery | No recovery action is required. |

35.44 ssh_user_logout

Table 761: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 762: 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: <i>\$fileName\$ \$reason\$</i> |
| 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 763: 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: <i>\$fileName\$</i> |
| Cause | Saving the LI configuration succeeded. |
| Effect | The LI configuration was saved. |
| Recovery | No recovery is necessary. |

35.47 ssiSyncConfigFailed

Table 764: 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 765: 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 tFiltrLiRsvdBlockRangeChangeEvent

Table 766: tFiltrLiRsvdBlockRangeChangeEvent properties

| Property name | Value |
|----------------------------------|---|
| Application name | LI |
| Event ID | 2038 |
| Event name | tFiltrLiRsvdBlockRangeChangeEvent |
| SNMP notification prefix and OID | TIMETRA-FILTER-MIB.tFilterNotifications.17 |
| Default severity | minor |
| Source stream | li |
| Message format string | LI Reserved Block <i>\$tLiReservedBlockName\$</i> range has changed (start-entry <i>\$tLiReservedBlockStart\$</i> size <i>\$tLiReservedBlockSize\$</i>). 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 767: 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 <i>\$tMirrorDestinationIndex\$</i> 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 tMirrorFilterAssignToltfWarn

Table 768: tMirrorFilterAssignToltfWarn properties

| Property name | Value |
|------------------|-------|
| Application name | LI |

| Property name | Value |
|----------------------------------|--|
| Event ID | 2030 |
| Event name | tMirrorFilterAssignToIrfWarn |
| SNMP notification prefix and OID | TIMETRA-MIRROR-MIB.tMirrorNotifications.19 |
| Default severity | minor |
| Source stream | li |
| Message format string | <i>\$tMirrorFilterType\$</i> filter <i>\$tMirrorFilterId\$</i> , which is referred to by Lawful Intercept has been applied on <i>\$tMirrorFilterDirection\$</i> to interface <i>\$tMirrorFilterIfName\$</i> (IfIndex <i>\$tMirrorFilterIfIndex\$</i>) |
| 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 769: 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 | <i>\$tMirrorFilterType\$</i> filter <i>\$tMirrorFilterId\$</i> , which is referred to by Lawful Intercept has been applied on <i>\$tMirrorFilterDirection\$</i> to SAP <i>\$tMirrorFilterSapEncapValue\$</i> in service <i>\$tMirrorFilterSvclid\$</i> |
| 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 770: 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 | <i>\$tMirrorFilterType\$</i> filter <i>\$tMirrorFilterId\$</i> , which is referred to by Lawful Intercept has been applied on <i>\$tMirrorFilterDirection\$</i> to SDP <i>\$tMirrorFilterSdpBindId\$</i> in service <i>\$tMirrorFilterSvcId\$</i> |
| 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 tMirrorLiFitrUnavailSath

Table 771: tMirrorLiFitrUnavailSath properties

| Property name | Value |
|------------------|-------|
| Application name | LI |
| Event ID | 2046 |

| Property name | Value |
|----------------------------------|--|
| Event name | tMirrorLiFiltrUnavailSath |
| SNMP notification prefix and OID | TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.3 |
| Default severity | minor |
| Source stream | li |
| Message format string | Lawful Intercept (LI) mirror source <i>\$tMirrorSourceIndex\$</i> SAP matching entry <i>\$tMirrorSourceFilterEntryId\$</i> of filter <i>\$tMirrorSourceFilterId\$</i> 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 tMirrorLiFiltrUnavailSathClr

Table 772: tMirrorLiFiltrUnavailSathClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | LI |
| Event ID | 2047 |
| Event name | tMirrorLiFiltrUnavailSathClr |
| SNMP notification prefix and OID | TIMETRA-MIRROR-MIB.tMirrorLiOamSathNotifs.4 |
| Default severity | minor |
| Source stream | li |
| Message format string | Lawful Intercept (LI) mirror source <i>\$tMirrorSourceIndex\$</i> SAP matching entry <i>\$tMirrorSourceFilterEntryId\$</i> of filter <i>\$tMirrorSourceFilterId\$</i> 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 773: 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 <i>\$tMirrorSourceIndex\$</i> LSN NAT64 subscriber (<i>\$vRtrID\$, \$tMirrorLiNatLsnSubAddr\$/tMirrorLiNatLsnSubPrefixLength\$</i>) changed to <i>\$tMirrorLiNat64SubOperState\$</i> |
| 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 774: 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 <i>\$tMirrorSourceIndex\$</i> I2-aware subscriber <i>\$tMirrorLiNatL2awSubIdent\$</i> changed to <i>\$tMirrorLiNatL2awSubOperState\$</i> |
| 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 775: 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 <i>\$tMirrorSourceIndex\$</i> LSN subscriber (<i>\$vRtrID\$</i> , <i>\$tMirrorLiNatLsnSubAddr\$</i> / <i>\$tMirrorLiNatLsnSubPrefixLength\$</i>) changed to <i>\$tMirrorLiNatLsnSubOperState\$</i> |

| 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 776: 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 <i>\$tMirrorNotifyLiSvcId\$</i> associated port <i>\$tMirrorNotifyLiPortId\$</i> 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 777: 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 <i>\$tMirrorNotifyLiSvcId\$</i> associated port <i>\$tMirrorNotifyLiPortId\$</i> 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 778: 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 <i>\$tMirrorNotifyLiSvcId\$</i> associated SAP <i>\$tMirrorNotifyLiSapEncapValue\$</i> 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 779: 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 780: 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: <i>\$tMirrorSourcePortLicenseState\$</i> |
| 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 tMirrorLiUpleInvalid

Table 781: tMirrorLiUpleInvalid properties

| Property name | Value |
|----------------------------------|--|
| Application name | LI |
| Event ID | 2043 |
| Event name | tMirrorLiUpleInvalid |
| 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 - <i>\$tMirrorLiNotifyLongDescription\$</i> |
| 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 782: 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 <i>\$tMirrorNotifyLiIdentifier\$</i> intercept-id= <i>\$tMirrorNotifyLiInterceptionId\$</i> session-id= <i>\$tMirrorNotifyLiSessionId\$</i> failed - <i>\$tMirrorLiNotifyLongDescription\$</i> |
| 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 783: 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 <i>\$tMirrorNotifyLiIdentifier\$</i> intercept-id= <i>\$tMirrorNotifyLiInterceptionId\$</i> session-id= <i>\$tMirrorNotifyLiSessionId\$</i> 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 784: 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 <i>\$tMirrorLiNotifyInIdentifier\$</i> <i>\$tMirrorLiNotifyX2AlarmRank\$</i> X2 alarm <i>\$tMirrorLiNotifyX2AlarmFlag\$</i> at <i>\$tMirrorLiNotifyDateAndTime\$</i> : <i>\$tMirrorLiNotifyLongDescription\$</i> |
| 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 785: 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 786: 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. <i>\$tMirrorSourceFilterDescr\$</i> |
| 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 787: 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. <i>\$tMirrorSourceFilterDescr\$</i> |
| 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 788: 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. <i>\$tMirrorSourceFilterDescr\$</i> |
| 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 tMirrorSourceIPFiltrChangeReject

Table 789: tMirrorSourceIPFiltrChangeReject properties

| Property name | Value |
|------------------|-------|
| Application name | LI |

| Property name | Value |
|----------------------------------|---|
| Event ID | 2020 |
| Event name | tMirrorSourceIPFtrChangeReject |
| 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 <i>\$tMirrorSourceFilterEntryId\$</i> of IP filter <i>\$tMirrorSourceFilterId\$</i> which is being referred to by Lawful Intercept (mirror-source <i>\$tMirrorSourceIndex\$</i>) |
| 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 tMirrorSourceIPv6FtrChangeRej

Table 790: tMirrorSourceIPv6FtrChangeRej properties

| Property name | Value |
|----------------------------------|---|
| Application name | LI |
| Event ID | 2033 |
| Event name | tMirrorSourceIPv6FtrChangeRej |
| 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 <i>\$tMirrorSourceFilterEntryId\$</i> of IPv6 filter <i>\$tMirrorSourceFilterId\$</i> which is being referred to by Lawful Intercept (mirror-source <i>\$tMirrorSourceIndex\$</i>) |
| Cause | The tMirrorSourceIPv6FtrChangeRej 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 791: 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. <i>\$tMirrorSourceFilterDescr\$</i> |
| 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 792: 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 <i>\$tMirrorSourceIndex\$</i> subscriber <i>\$tMirrorSourceSubIdent\$</i> on SAP <i>\$tMirrorNotifyLiSapEncap Value\$</i> in service <i>\$tMirrorNotifyLiSvcId\$</i> could not be intercepted -- <i>\$tMirrorNotifyLiDescription\$</i> |
| 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 tMirrorSourceMacFiltrChangeReject

Table 793: tMirrorSourceMacFiltrChangeReject properties

| Property name | Value |
|----------------------------------|--|
| Application name | LI |
| Event ID | 2021 |
| Event name | tMirrorSourceMacFiltrChangeReject |
| 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 <i>\$tMirrorSourceFilterEntryId\$</i> of Mac filter <i>\$tMirrorSourceFilterId\$</i> which is being referred to by Lawful Intercept (mirror-source <i>\$tMirrorSourceIndex\$</i>) |
| 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 794: 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 <i>\$tmnxClearName\$</i> has been run with parameters: <i>\$tmnxClearParams\$</i> . The completion result is: <i>\$tmnxClearResult\$</i> . Additional error text, if any, is: <i>\$tmnxClearErrorText\$</i> |
| 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 795: *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 | <i>\$tmnxNotifyObjectName\$</i> 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 796: *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 | <i>\$tmnxNotifyObjectName\$</i> 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 797: 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 | <i>\$tmnxNotifyObjectName\$</i> 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 798: 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 <i>\$tmnxNotifyObjectName\$</i> changed administrative state: <i>\$tmnxNotifyRowAdminState\$</i> , operational state: <i>\$tmnxNotifyRowOperState\$</i> |
| 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 IldpRemTablesChange

Table 799: IldpRemTablesChange properties

| Property name | Value |
|----------------------------------|--|
| Application name | LLDP |
| Event ID | 2001 |
| Event name | IldpRemTablesChange |
| SNMP notification prefix and OID | LLDP-MIB.IldpNotificationPrefix.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 800: 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 <i>\$ifIndex\$</i> , dest-mac-type <i>\$tmnxLldpRemLocalDestMACAddress\$</i> , remote system name <i>\$tmnxLldpRemSysName\$</i> , remote chassis-id <i>\$tmnxLldpRemChassisId\$</i> , remote port-id <i>\$tmnxLldpRemPortId\$</i> , remote-index <i>\$tmnxLldpRemIndex\$</i> |
| 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 801: 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 <i>\$ifIndex\$</i> , dest-mac-type <i>\$tmnxLldpRemLocalDestMACAddress\$</i> , remote system name <i>\$tmnxLldpRemSysName\$</i> , remote chassis-id <i>\$tmnxLldpRemChassisId\$</i> , remote port-id <i>\$tmnxLldpRemPortId\$</i> , remote-index <i>\$tmnxLldpRemIndex\$</i> |
| 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 802: 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 <i>\$ifIndex\$</i> , dest-mac-type <i>\$tmnxLldpRemLocalDestMACAddress\$</i> , remote system name <i>\$tmnxLldpRemSysName\$</i> , remote chassis-id <i>\$tmnxLldpRemChassisId\$</i> , remote port-id <i>\$tmnxLldpRemPortId\$</i> , remote-index <i>\$tmnxLldpRemIndex\$</i> |
| Cause | The tmnxLldpRemEntryPeerUpdated notification is generated when a tmnxLldpRemSysName changes for an existing peer |
| Effect | N/A |
| Recovery | N/A |

36.5 tmnxLldpRemManAddrEntryAdded

Table 803: 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 <i>\$ifIndex\$</i> , dest-mac-type <i>\$tmnxLldpRemLocalDestMACAddress\$</i> , remote management address <i>\$tmnxLldpRemManAddr\$</i> , remote-index <i>\$tmnxLldpRemIndex\$</i> |
| Cause | The <i>tmnxLldpRemManAddrEntryAdded</i> notification is generated when a remote management address is added to the LLDP |
| Effect | N/A |
| Recovery | N/A |

36.6 *tmnxLldpRemManAddrEntryRemoved*

Table 804: *tmnxLldpRemManAddrEntryRemoved* properties

| Property name | Value |
|----------------------------------|--|
| Application name | LLDP |
| Event ID | 2105 |
| Event name | <i>tmnxLldpRemManAddrEntryRemoved</i> |
| SNMP notification prefix and OID | TIMETRA-LLDP-MIB. <i>tmnxLldpNotifs.5</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | LLDP Remote peer mgmt address removed, local-port-id <i>\$ifIndex\$</i> , dest-mac-type <i>\$tmnxLldpRemLocalDestMACAddress\$</i> , remote management address <i>\$tmnxLldpRemManAddr\$</i> , remote-index <i>\$tmnxLldpRemIndex\$</i> |
| Cause | The <i>tmnxLldpRemManAddrEntryRemoved</i> 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 805: 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 <i>\$taskName\$</i> 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 806: 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 <i>\$tmnxClearName\$</i> has been run with parameters: <i>\$tmnxClearParams\$</i> . The completion result is: <i>\$tmnxClearResult\$</i> . Additional error text, if any, is: <i>\$tmnxClearErrorText\$</i> |
| 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 807: 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 | <i>\$logCustomEventMessageString\$</i> |
| 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 808: 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 | <i>\$logCustomEventMessageString\$</i> |
| 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 809: 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 | <i>\$logCustomEventMessageString\$</i> |
| 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 810: 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 | <i>\$logCustomEventMessageString\$</i> |
| 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 811: *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 | <i>\$logCustomEventMessageString\$</i> |
| 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 812: *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 | <i>\$logCustomEventMessageString\$</i> |
| 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 813: *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 <i>\$subject\$</i> . |
| 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 814: *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: <ul style="list-style-type: none"> • Compact flash location is not available for <i>\$subject\$</i>. Backup location, if any, will be used. • Compact flash location of <i>\$tmnxLogFileIdAdminLocation\$</i> is not available for <i>\$subject\$</i>. 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 815: *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 816: 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 817: 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 | <i>\$tmnxLogThrottledEvents\$ \$tmnxLogThrottledEventID\$</i> 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 818: 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 <i>\$tmnxLogFileDeletedName\$</i> on compact flash cf <i>\$tmnxLogFileDeletedLocation\$</i> 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 819: 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 <i>\$tmnxLogFileIdPathName\$</i> on compact flash cf <i>\$tmnxLogFileIdOperLocation\$</i> has been rolled over |
| Cause | Generated when an event log or accounting policy file's rollover time has expired. |
| Effect | The file located as indicated by the value of tmnxLogFileIdOper Location is closed and a new file is created as specified by tmnxLogFileIdAdminLocation and tmnxLogFileIdBackupLoc. |
| Recovery | No recovery is necessary. |

37.16 tmnxLogOnlyEventOverrun

Table 820: 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 | <i>\$tmnxLogOnlyOverrunEvents\$ \$tmnxLogOnlyOverrunEventName\$</i> 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 821: *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 | <i>\$tmnxLogOnlyThrottledEvents\$ \$tmnxLogOnlyThrottledEventName\$</i> 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 <i>tmnxLogOnlyEventThrottled</i> 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 822: *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 <i>\$cFlashId\$</i> during I/O for <i>\$subject\$</i> . |

| 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 823: 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 | <i>\$tmnxLogTraceErrorTitle\$</i> : <i>\$tmnxLogTraceErrorMessage\$</i> |
| 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 tmnxNetconfNotifyOverrun

Table 824: *tmnxNetconfNotifyOverrun* properties

| Property name | Value |
|----------------------------------|--|
| Application name | LOGGER |
| Event ID | 2030 |
| Event name | tmnxNetconfNotifyOverrun |
| SNMP notification prefix and OID | TIMETRA-LOG-MIB.tmnxLogNotifications.19 |
| Default severity | major |
| Source stream | main |
| Message format string | Netconf Notify Queue for Netconf stream <i>\$tmnxLogIdNetconfStream\$</i> was overrun. Packet drop count <i>\$tmnxNetconfStreamDropCount\$</i> |
| Cause | A <i>tmnxNetconfNotifyOverrun</i> notification is generated when Netconf Notify queue is overrun. This queue is responsible for sending log events into Netconf servers as Netconf Notifications. Link to Netconf server is too slow for current log event rate or link to Netconf server is down. |
| Effect | Logger events have been dropped and were not sent to particular Netconf stream destination. |
| Recovery | Use faster link to Netconf server, or implement throttle policies, to decrease number of reported events. |

37.21 *tmnxStdEventsReplayed*

Table 825: *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 |

| Property name | Value |
|-----------------------|--|
| Message format string | Events <i>\$tmnxStdReplayStartEvent\$</i> to <i>\$tmnxStdReplayEndEvent\$</i> from <i>\$subject\$</i> have been resent to SNMP notification target address <i>\$tmnxStdDestAddr\$</i> . The first event with no route to the target address was <i>\$tmnxStdReplayStart\$</i> . |
| 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 <i>tmnxStdEventsReplayed</i> notification is generated when an SNMP trap target address is added to the RTM (<i>tmnxVRtrID</i>) following a period when the address had been removed. The value of <i>tmnxStdReplayStartEvent</i> is the SNMP notification request ID of the first event that was replayed. The value of <i>tmnxStdReplayEndEvent</i> is the SNMP notification request ID of the last missed event that was replayed. The value of <i>tmnxStdReplayStart</i> is the request ID of the first event for which there was no route to the trap target address. |
| Recovery | N/A |

37.22 tmnxSysLogTargetProblem

Table 826: *tmnxSysLogTargetProblem* properties

| Property name | Value |
|----------------------------------|--|
| Application name | LOGGER |
| Event ID | 2013 |
| Event name | <i>tmnxSysLogTargetProblem</i> |
| SNMP notification prefix and OID | TIMETRA-LOG-MIB. <i>tmnxLogNotifications.9</i> |
| Default severity | major |
| Source stream | main |
| Message format string | Problem encountered when trying to reach the destination specified in syslog <i>\$tmnxSysLogTargetId\$</i> : <i>\$tmnxSysLogTargetProblemDescr\$</i> . |
| Cause | An event could not be delivered to the destination specified for the syslog. |
| Effect | A <i>tmnxSysLogTargetProblem</i> notification is generated when a problem is encountered when trying to deliver data to the syslog destination identified by the <i>tmnxSysLogTargetId</i> . |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

37.23 tmnxTestEvent

Table 827: *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 | <p>Possible messages:</p> <ul style="list-style-type: none"> • Test event has been generated with system object identifier <i>\$sys ObjectID\$</i> System description: <i>\$sysDescr\$</i> • <i>\$tmnxLogEventTestCustomText\$</i> |
| Cause | The tmnxTestEvent notification is generated when the object tmnx EventTest is set to a value of 'doAction' or the tools>perform>log>test-event CLI command has been entered. This event can be used to test that remote log destinations such as syslog and snmp trap destinations are configured correctly. |
| Effect | A tmnxTestEvent is generated. |
| Recovery | If the test event is not received by the log destination, verify that syslog and snmp trap destinations are configured correctly and that the interface link between the system and the remote receiver is up. |

38 MACSEC

38.1 tmnxMacsecCaCreate

Table 828: 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 \$tmnxMacsecPreSharedKeyIndex\$ 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 829: 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.tmnxMacsecNofitations.1 |
| Default severity | minor |
| Source stream | main |
| Message format string | MACsec CA <i>\$tmnxMacsecConnAssocName\$</i> CKN <i>\$tmnxMacsecPreSharedKeyCakName\$</i> configured on port <i>\$tmnxMacsecNotifyPortId\$</i> sub-port <i>\$tmnxMacsecNotifyVlanId\$</i> |
| Cause | A <i>tmnxMacsecConfiguredPortCA</i> notification is generated when a CA is associated with a port. |
| Effect | N/A |
| Recovery | N/A |

38.3 tmnxMacsecDisabledPort

Table 830: *tmnxMacsecDisabledPort* properties

| Property name | Value |
|----------------------------------|---|
| Application name | MACSEC |
| Event ID | 2004 |
| Event name | <i>tmnxMacsecDisabledPort</i> |
| SNMP notification prefix and OID | TIMETRA-MACSEC-MIB.tmnxMacsecNofitations.4 |
| Default severity | minor |
| Source stream | main |
| Message format string | MACsec admin disabled on port <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecNotifyVlanId\$</i> CA <i>\$tmnxMacsecPortCaName\$</i> |
| Cause | A <i>tmnxMacsecDisabledPort</i> 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 831: *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 <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecVlanId\$</i> RxSCI <i>\$tmnxMacsecRxSci\$</i> data packets replay count <i>\$tmnxMacsecRxSCStatsLatePkts\$</i> |
| 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 832: *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 <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecNotifyVlanId\$</i> CA <i>\$tmnxMacsecPortCaName\$</i> |
| Cause | A <i>tmnxMacsecEnabledPort</i> 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 833: *tmnxMacsecMaxPeerLimitCleared* properties

| Property name | Value |
|----------------------------------|--|
| Application name | MACSEC |
| Event ID | 2010 |
| Event name | <i>tmnxMacsecMaxPeerLimitCleared</i> |
| SNMP notification prefix and OID | TIMETRA-MACSEC-MIB. <i>tmnxMacsecNofitications.10</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | MACsec peer limit cleared on security-zone <i>\$tmnxMacsecNotifySecurityZone\$</i> for peer <i>mi:mac \$tmnxMacsecNotifyPeerMi:\$tmnxMacsecMkaPeerListSci\$</i> on port <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecVlanId\$</i> |
| Cause | A <i>tmnxMacsecMaxPeerLimitCleared</i> 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 834: *tmnxMacsecMaxPeerLimitExceeded* properties

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

38.8 tmnxMacsecMkaReplayAttemptDisc

Table 835: *tmnxMacsecMkaReplayAttemptDisc* properties

| Property name | Value |
|----------------------------------|---|
| Application name | MACSEC |
| Event ID | 2015 |
| Event name | tmnxMacsecMkaReplayAttemptDisc |
| SNMP notification prefix and OID | TIMETRA-MACSEC-MIB.tmnxMacsecNotifications.15 |
| Default severity | minor |
| Source stream | main |
| Message format string | MACsec CA <i>\$tmnxMacsecPortCaName\$</i> port <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecVlanId\$</i> MACsec MKA packets replay count <i>\$tmnxMacsecMkaStatsPdInvalidNum\$</i> |

| 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 836: 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 \$tmnxMacsecNotifyAssociationNum\$ |
| 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 837: *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 838: *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 |
|---------------|---|
| | <i>\$tmnxMacsecNotifyVlanId\$</i> new SAK installed AN <i>\$tmnxMacsecNotifyAssociationNum\$</i> |
| Cause | A <i>tmnxMacsecSakInstalledRx</i> notification is generated when a new SAK is installed for receiving |
| Effect | N/A |
| Recovery | N/A |

38.12 tmnxMacsecSakInstalledTx

Table 839: *tmnxMacsecSakInstalledTx* properties

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

38.13 tmnxMacsecUnconfiguredPortCA

Table 840: *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 <i>\$tmnxMacsecConnAssocName\$</i> CKN <i>\$tmnxMacsecPreSharedKeyCakName\$</i> unconfigured on port <i>\$tmnxMacsecNotifyPortId\$</i> sub-port <i>\$tmnxMacsecNotifyVlanId\$</i> |
| Cause | A tmnxMacsecUnconfiguredPortCA notification is generated when a CA is unassociated from a port. |
| Effect | N/A |
| Recovery | N/A |

38.14 tmnxMkaOperStateChanged

Table 841: *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: <i>\$tmnxMacsecMkaStatsOperState\$</i> on port <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecVlanId\$</i> CA <i>\$tmnxMacsecPortCaName\$</i> |

| 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 842: 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 843: 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 <i>\$tmnxMacsecMkaPeerListMi\$</i> : <i>\$tmnxMacsecMkaPeerListSci\$</i> on port <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecVlanId\$</i> CA <i>\$tmnxMacsecPortCaName\$</i> local MI <i>\$tmnxMacsecMkaStatsMemberId\$</i> |
| Cause | A tmnxMkaSessionEnded notification is generated when an MKA session is ended. |
| Effect | N/A |
| Recovery | N/A |

38.17 tmnxMkaSessionEstablished

Table 844: *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 <i>\$tmnxMacsecMkaPeerListMi\$</i> : <i>\$tmnxMacsecMkaPeerListSci\$</i> on port <i>\$tmnxMacsecPortId\$</i> sub-port <i>\$tmnxMacsecVlanId\$</i> CA <i>\$tmnxMacsecPortCaName\$</i> EAPOL-destination <i>\$tmnxMacsecPortEapolDestAddress\$</i> local key-server priority <i>\$tmnxMacsecMkaStatsKeyServerPrio\$</i> peer key-server priority <i>\$tmnxMacsecStaticCakKeyServerPrio\$</i> cipher-suite <i>\$tmnxMacsecConnAssocCipherSuite\$</i> encryption offset <i>\$tmnxMacsecConnAssocEnchrptnOffset\$</i> localMI <i>\$tmnxMacsecMkaStatsMemberId\$</i> |

| 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 845: 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 <i>\$tmnxMcPeerSrcIpAddr\$</i> because <i>\$srrpPacketDiscardReason\$</i> |
| 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 846: 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 <i>\$tMcIPsecDomainId\$</i> local activity state changed from <i>\$tMcIPsecDomainActyStateOld\$</i> to <i>\$tMcIPsecDomain ActivityState\$</i> because <i>\$tMcIPsecDomainActyStateChR\$</i> , and the active router in the domain is <i>\$tMcIPsecDmCurActiveRouterId\$</i> |
| 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 tMcIpssecDomainProtStatusChg

Table 847: tMcIpssecDomainProtStatusChg properties

| Property name | Value |
|----------------------------------|---|
| Application name | MC_REDUNDANCY |
| Event ID | 2047 |
| Event name | tMcIpssecDomainProtStatusChg |
| 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 <i>\$tMcIPsecDomain Id\$</i> changed to <i>\$tMcIPsecDomainProtectStatus\$</i> |
| 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 848: 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 <i>\$tmnxMcPeerIpAddr\$</i> tunnel-group <i>\$tMcPeerIPsecTnlGrpId\$</i> changed from <i>\$tMcPeerIPsecTnlGrpMasterStateOld\$</i> to <i>\$tMcPeerIPsecTnlGrpMasterState\$</i> because <i>\$tMcPeerIPsecTnlGrpMasterStateChR\$</i> |
| 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 849: 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 <i>\$tmnxMcPeerIpAddr</i> \$ tunnel-group <i>\$tMcPeerIPsecTnlGrpId</i> changed to <i>\$tMcPeerIPsecTnlGrpProtectStatus</i> |
| 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 850: 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 <i>\$tmnxMcPeerIpAddr\$</i> with source <i>\$tmnxMcPeerSrcIpAddr\$</i> 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 851: *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 <i>\$tmnxMcPeerIpAddr\$</i> with source <i>\$tmnxMcPeerSrcIpAddr\$</i> is enabled. Passive-mode with peer has <i>\$tmnxMcPeerEPPsvModeConfigState\$</i> |
| 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 852: *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 <i>\$tmnxMcPeerIpAddrForNotify\$</i> configuration changed. |
| Cause | Entries in tmnxMcLagInfoLagTable were changed. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

39.9 tmnxMcOmcrClientNumEntriesHigh

Table 853: *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 <i>\$tmnxMcsClientApplication\$</i> is becoming too high: <i>\$tmnxMcNotifyNumber\$%</i> (peer <i>\$tmnxMcPeerIpAddr\$</i>) |
| Cause | The notification <i>tmnxMcOmcrClientNumEntriesHigh</i> 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 <i>tmnxMcPeerWarmStandby</i> 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 <i>tmnxMcsClientNumEntries</i> for the client application specified by <i>tmnxMcsClientApplication</i> . The maximum number of entries for a client application is equal to one million. The value of <i>tmnxMcNotifyNumber</i> 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 <i>tmnxMcPeerIpType</i> and <i>tmnxMcPeerIpAddr</i> 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 <i>tmnxMcPeerIpType</i> and <i>tmnxMcPeerIpAddr</i> is shut down automatically by this system (the value of <i>tmnxMcPeerSyncAdminState</i> is set to 'out OfService' and the value of <i>tmnxMcPeerSyncOperFlags</i> 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 854: *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 | <i>\$tmnxMcOmcrStatClientApplication\$</i> OMCR protection with <i>\$tmnxMcOmcrStatAccessProtection\$</i> instance <i>\$tmnxMcOmcrStatIndex\$</i> <i>\$tmnxMcOmcrStatFailed\$</i> - <i>\$tmnxMcOmcrStatFailure\$</i> |
| Cause | The notification <i>tmnxMcOmcrStatFailedChanged</i> is generated when the value of the object <i>tmnxMcOmcrStatFailed</i> 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 <i>tmnxMcOmcrStatFailed</i> 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 <i>tmnxSrrpOperState</i> 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 855: *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 <i>\$tmnxMcPeerIpAddr\$</i> with source <i>\$tmnxMcPeerSrcIpAddr\$</i> |
| 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 856: *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 <i>\$tmnxMcPeerIpAddr\$</i> and source <i>\$tmnxMcPeerSrcIpAddr\$</i> 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 857: 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 <i>\$tmnxMcPeerIpAddr\$</i> and source <i>\$tmnxMcPeerSrcIpAddr\$</i> with status= <i>\$tmnxMcPeerEPBfdSessionOpenStatus\$</i> |
| 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 858: 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 <i>\$tmnxMcPeerIpAddr\$</i> and source <i>\$tmnxMcPeerSrcIpAddr\$</i> 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 859: *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 <i>\$tmnxMcPeerIpAddr\$</i> with source <i>\$tmnxMcPeerSrcIpAddr\$</i> 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 860: *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 <i>\$tmnxMcPeerSrcIpAddr\$</i> with source <i>\$tmnxMcPeerIpAddr\$</i> 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 861: *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 <i>\$tmnxMcPeerIpAddr\$</i> changed to <i>\$tmnxMcPeerRingsOperState\$</i> . |

| Property name | Value |
|---------------|---|
| Cause | The notification <code>tmnxMcPeerRingsOperStateChanged</code> is sent when the operational state, with respect to multi-chassis ring operation, of a peer changed. <code>unknown</code> No rings are configured for this peer. <code>inService</code> The signaling connection for mc-ring operation is operational. <code>outOfService</code> The signaling connection for mc-ring operation has timed out. <code>transition</code> Not implemented. |
| Effect | <code>unknown</code> None. <code>inService</code> The signaling connection for mc-ring operation is operational. <code>outOfService</code> 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. <code>transition</code> Not implemented. |
| Recovery | The recovery depends on the operational state of the ring: <code>unknown</code> None. <code>inService</code> None. <code>outOfService</code> Restore the IP connectivity between the local peer and the remote peer. <code>transition</code> Not implemented. |

39.18 `tmnxMcPeerSyncStatusChanged`

Table 862: `tmnxMcPeerSyncStatusChanged` properties

| Property name | Value |
|----------------------------------|--|
| Application name | MC_REDUNDANCY |
| Event ID | 2004 |
| Event name | <code>tmnxMcPeerSyncStatusChanged</code> |
| SNMP notification prefix and OID | TIMETRA-MC-REDUNDANCY-MIB. <code>tmnxMcRedundancyNotifications.4</code> |
| Default severity | warning |
| Source stream | main |
| Message format string | The Sync status of peer <code>\$tmnxMcPeerIpAddr\$</code> changed to <code>\$tmnxMcPeerSyncStatus\$</code> |
| Cause | The event is generated when the sync state changes. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

39.19 tmnxMcRedundancyMismatchDetected

Table 863: *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 | <i>\$tmnxMcLagConfigMismatchString\$</i> |
| Cause | The event is generated when a configuration mismatch is detected. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

39.20 tmnxMcRedundancyMismatchResolved

Table 864: *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 | <i>\$tmnxMcLagConfigMismatchString\$</i> |
| 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 865: *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 <i>\$tmnxMcPeerIpAddr\$</i> changed to <i>\$tmnxMcLagConfigOperState\$</i> |
| 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 866: *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 <i>\$tmnxMcPeerIpAddr\$:: \$tmnxMcPeerSyncPortSyncTag\$</i> changed to <i>\$tmnxMcRingInfoOperState\$</i> . |
| Cause | The notification <i>tmnxMcRingInbCtrlOperStateChgd</i> 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 867: *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 <i>\$tmnxMcPeerIpAddr\$:: \$tmnxMcPeerSyncPortSyncTag\$:: \$tmnxMcRingNodeName\$</i> changed to <i>\$tmnxMcRingNodeInfoLocOperState\$</i> while in-use is <i>\$tmnxMcRingNodeInfoInUse\$</i> . |

| 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 868: 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 869: 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 | <i>\$tmnxMcPeerSyncClient\$ back in sync with peer \$tmnxMcPeerIpAddrForNotify\$.</i> |
| 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 870: *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 | <i>\$tmnxMcPeerSyncClient\$ lost sync with peer \$tmnxMcPeerIpAddrForNotify\$.</i> |
| 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 871: *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 <i>\$tmnxMcPeerIpAddrForNotify\$</i> differs <i>\$tmnxMcPeerClockSkew\$</i> 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 872: *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 <i>\$tmnxMcPeerIpAddrForNotify\$</i> differs <i>\$tmnxMcPeerClockSkew\$</i> 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 873: 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 <i>\$tmnxSrrpOperID\$</i> on interface <i>\$vRtrIfIndex\$</i> changed state to backup - current master is <i>\$tmnxMcPeerIpAddrForNotify\$</i> |
| Cause | The sending agent has transitioned to 'Backup' state. |
| Effect | N/A |
| Recovery | N/A |

39.30 tmnxSrrpBfdIntfSessStateChgd

Table 874: *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 <i>\$tmnxSrrpNotifBfdIntfSvcId\$</i> interface <i>\$tmnxSrrpNotifBfdIntfName\$</i> to peer <i>\$tmnxSrrpNotifBfdIntfDestIp\$</i> changed state to <i>\$tmnxSrrpNotifBfdIntfSessState\$</i> . |
| Cause | The operational state of BFD session of the SRRP instance changed. |
| Effect | N/A |
| Recovery | N/A |

39.31 tmnxSrrpDualMaster

Table 875: *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 <i>\$tmnxSrrpOperID\$</i> : Dual Master detected on both peer <i>\$tmnxMcPeerIpAddrForNotify\$</i> / interface <i>\$tmnxMcRemoteGrpIfNameForNotify\$</i> and local <i>\$tmnxMcPeerSrcIpAddr\$</i> / interface <i>\$vRtrIfIndex\$</i> . |

| 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 876: 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 <i>\$tmnxSrrpOperID\$</i> : IP Address on interface <i>\$vRtrIfIndex\$</i> on local node <i>\$tmnxMcPeerSrcIpAddr\$</i> conflicts with IP Address on node <i>\$tmnxMcPeerIpAddrForNotify\$</i> . |
| 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 tmnxSrrpInstanceldMismatch

Table 877: tmnxSrrpInstanceldMismatch 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 <i>\$tmnxMcPeerIpAddrForNotify\$</i> did not match srrp <i>\$tmnxSrrpOperID\$</i> on local node <i>\$tmnxMcPeerSrcIpAddr\$</i> : interface <i>\$vRtrIfIndex\$</i> . |
| 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 878: tmnxSrrpOperDownInvalidMac properties

| Property name | Value |
|----------------------------------|--|
| Application name | MC_REDUNDANCY |
| Event ID | 2043 |
| Event name | tmnxSrrpOperDownInvalidMac |
| SNMP notification prefix and OID | TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.39 |
| Default severity | minor |
| Source stream | main |
| Message format string | tmnxSrrpOperDownInvalidMac notification from SRRP id <i>\$tmnxSrrpOperID\$</i> on interface <i>\$vRtrIfIndex\$</i> . 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 879: 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 <i>\$tmnxSrrp OperID\$</i> on interface <i>\$vRtrIfIndex\$</i> 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 880: *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 <i>\$tmnxSrrpOperID\$</i> : mismatch in private retail configuration for service <i>\$tmnxMcNotifyServiceId\$</i> <i>\$tmnxMcNotifyTruthValue\$</i> detected/resolved |
| Cause | The notification <i>tmnxSrrpPrivRetailMismatch</i> is generated with a value of 'true' for <i>tmnxMcNotifyServiceId</i> 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 881: *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 <i>\$tmnxSrrpOperID\$</i> : Redundant interface <i>\$tmnxMcRemoteRedIfNameForNotify\$</i> on peer <i>\$tmnxMcPeerIpAddrForNotify\$</i> / interface <i>\$tmnxMcRemoteGrpIfNameForNotify\$</i> does not match local <i>\$tmnxMcPeerSrcIpAddr\$</i> / interface <i>\$vRtrIfIndex\$</i> . |
| Cause | The local and remote redundant interfaces are not properly paired. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

39.38 tmnxSrrpSapMismatch

Table 882: *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 <i>\$tmnxSrrpOperID\$</i> : SAPs on peer interface <i>\$tmnxMcRemoteGrpIfNameForNotify\$</i> do not match those on local interface <i>\$vRtrIfIndex\$</i> . |
| 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 883: *tmnxSrrpSapTagMismatch* properties

| Property name | Value |
|----------------------------------|---|
| Application name | MC_REDUNDANCY |
| Event ID | 2011 |
| Event name | tmnxSrrpSapTagMismatch |
| SNMP notification prefix and OID | TIMETRA-MC-REDUNDANCY-MIB.tmnxMcRedundancyNotifications.11 |
| Default severity | warning |
| Source stream | main |
| Message format string | SRRP ID <i>\$tmnxSrrpOperID\$</i> : SAP encap of <i>\$sapEncapValue\$</i> on peer interface <i>\$tmnxMcRemoteGrplfNameForNotify\$</i> has MCS tag <i>\$tmnxMcRemoteSyncTag\$</i> , which differs from local tag <i>\$tmnxMcPeerSyncPortEncapSyncTag\$</i> on interface <i>\$vRtrIfIndex\$</i> . |
| 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 884: *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 <i>\$tmnxMcPeerIpAddrForNotify\$</i> did not match the address list configured for SRRP instance <i>\$tmnxSrrpOperID\$</i> on local node <i>\$tmnxMcPeerSrcIpAddr\$</i> : interface <i>\$vRtrIfIndex\$</i> . |

| 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 885: 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 <i>\$tmnxMcPeerIpAddrForNotify\$</i> matched the address list configured for SRRP instance <i>\$tmnxSrrpOperID\$</i> on local node <i>\$tmnxMcPeerSrcIpAddr\$</i> : interface <i>\$vRtrIfIndex\$</i> . |
| 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 886: *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 887: *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 <i>\$tmnxSrrpOperID\$</i> on interface <i>\$vRtrIfIndex\$</i> (primary address <i>\$tmnxMcPeerIpAddrForNotify\$</i>) 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 888: 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 <i>\$strTmnxMcPathChlPathType\$</i> path on slot/fp <i>\$tmnxMcPathCardSlotNum\$/\$tmnxMcPathFPNum\$</i> is within range limits. |
| Cause | The available bandwidth limit fell below the maximum limit. |
| Effect | N/A |
| Recovery | N/A |

40.2 tmnxMcPathAvailBwLimitExceeded

Table 889: 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 <i>\$strTmnxMcPathChlPathType\$</i> path on slot/fp <i>\$tmnxMcPathCardSlotNum\$/\$tmnxMcPathFPNum\$</i> has reached its maximum limit. |
| Cause | The available bandwidth limit has been reached. |
| Effect | N/A |
| Recovery | N/A |

40.3 tmnxMcPathSrcGrpBlackHole

Table 890: *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 (<i>\$tmnxMcPathChlSrcAddr\$,\$tmnxMcPathChlGrpAddr\$</i>) for <i>\$tmnxMcPathChlRtrType\$</i> instance <i>\$tmnxMcPathChlRtrInstance\$</i> slot/fp <i>\$tmnxMcPathCardSlotNum\$/\$tmnxMcPathFPNum\$</i> 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 891: *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 (<i>\$tmnxMcPathChlSrcAddr\$, \$tmnxMcPathChlGrpAddr\$</i>) for <i>\$tmnxMcPathChlRtrType\$</i> instance <i>\$tmnxMcPathChlRtrInstance\$</i> slot/ fp <i>\$tmnxMcPathCardSlotNum\$</i> / <i>\$tmnxMcPathFPNum\$</i> 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 892: *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 <i>\$operation-id\$</i> finished with status <i>\$status\$</i> . Presence of messages in the global operations table: error-messages <i>\$error-messages\$</i> , warning-messages <i>\$warning-messages\$</i> , info-messages <i>\$info-messages\$</i> . |
| Cause | Asynchronous operation finished its execution. |
| Effect | Full operation results are available. |
| Recovery | No recovery is required. |

41.2 mdAutomaticRollbackFailed

Table 893: *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 \$srcAddr\$ 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 894: 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 895: 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 896: 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 897: 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 898: 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 <i>\$userName\$</i> (<i>\$interface\$</i>) from <i>\$srcAddr\$</i> 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 899: 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 <i>\$operation-id\$</i> finished with status <i>\$status\$</i> . Presence of messages in the global operations table: error-messages <i>\$error-messages\$</i> , warning-messages <i>\$warning-messages\$</i> , info-messages <i>\$info-messages\$</i> . |
| Cause | Synchronous operation finished its execution. |
| Effect | Operation ID was freed. |
| Recovery | No recovery is required. |

42 MIRROR

42.1 destinationDisabled

Table 900: 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 <i>\$tMirrorDestinationIndex\$</i> 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 901: 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 <i>\$tMirrorDestinationIndex\$</i> 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 902: 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 <i>\$tMirrorSourceIndex\$</i> 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 903: 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 <i>\$tMirrorSourceIndex\$</i> 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 904: 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 <i>\$tMirrorSourceIndex\$</i> associated IP filter <i>\$tMirrorSourceFilterId\$</i> entry <i>\$tMirrorSourceFilterEntryId\$</i> has been <i>\$tMirrorSourceChangeType\$</i> |
| 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 905: 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 <i>\$tMirrorSourceIndex\$</i> associated MAC filter <i>\$tMirrorSourceFilterId\$</i> entry <i>\$tMirrorSourceFilterEntryId\$</i> has been <i>\$tMirrorSourceChangeType\$</i> |
| 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 906: 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 <i>\$tMirrorSourceIndex\$</i> associated SAP <i>\$tMirrorSource SapEncapValue\$</i> has been <i>\$tMirrorSourceChangeType\$</i> |
| 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 907: 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 <i>\$tMirrorSourceIndex\$</i> associated subscriber " <i>\$tMirrorSourceSubIdent\$</i> " has been <i>\$tMirrorSourceChangeType\$</i> |
| 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 tMirrorFiltrUnavailSath

Table 908: tMirrorFiltrUnavailSath properties

| Property name | Value |
|----------------------------------|---|
| Application name | MIRROR |
| Event ID | 2025 |
| Event name | tMirrorFiltrUnavailSath |
| SNMP notification prefix and OID | TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.3 |
| Default severity | minor |
| Source stream | main |
| Message format string | Mirror source <i>\$tMirrorSourceIndex\$</i> SAP matching entry <i>\$tMirrorSourceFilterEntryId\$</i> of filter <i>\$tMirrorSourceFilterId\$</i> 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 tMirrorFiltrUnavailSathClr

Table 909: *tMirrorFtrUnavailSathClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | MIRROR |
| Event ID | 2026 |
| Event name | tMirrorFtrUnavailSathClr |
| SNMP notification prefix and OID | TIMETRA-MIRROR-MIB.tMirrorOamSathNotifs.4 |
| Default severity | minor |
| Source stream | main |
| Message format string | Mirror source <i>\$tMirrorSourceIndex\$</i> SAP matching entry <i>\$tMirrorSourceFilterEntryId\$</i> of filter <i>\$tMirrorSourceFilterId\$</i> 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 910: *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 <i>\$tMirrorSourceIndex\$</i> associated port <i>\$tMirrorSourcePortIndex\$</i> 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 911: 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 <i>\$tMirrorSourceIndex\$</i> associated port <i>\$tMirrorSourcePort Index\$</i> 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 912: 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 <i>\$tMirrorSourceIndex\$</i> associated SAP <i>\$tMirrorSource SapEncapValue\$</i> 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 913: 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 <i>\$tMirrorSourceIndex\$</i> associated SAP <i>\$tMirrorSource SapEncapValue\$</i> 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 914: 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 <i>\$tMirrorSourceIndex\$</i> associated IPv6 filter <i>\$tMirrorSourceFilterId\$</i> entry <i>\$tMirrorSourceFilterEntryId\$</i> has been <i>\$tMirrorSourceChangeType\$</i> |
| Cause | The tMirrorSourceIpv6FilterChange event is generated when a IPv6 filter or filter entry associated with the mirror-source indicated by tMirrorSourceIndex 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 vRtrMldGrplfSapCModeRxQueryMism

Table 915: vRtrMldGrplfSapCModeRxQueryMism properties

| Property name | Value |
|----------------------------------|--|
| Application name | MLD |
| Event ID | 2015 |
| Event name | vRtrMldGrplfSapCModeRxQueryMism |
| SNMP notification prefix and OID | TIMETRA-MLD-MIB.vRtrMldNotifications.15 |
| Default severity | warning |
| Source stream | main |
| Message format string | Compatible mode oper version <i>\$vRtrMldGrplfSapOperVersion\$</i> mismatches query version <i>\$vRtrMldNotifyQueryVersion\$</i> |
| Cause | A vRtrMldGrplfSapCModeRxQueryMism 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. vRtrMldGrplfSapOperVersion 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 vRtrMldGrplfSapMaxGrpsLimExceed

Table 916: 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 vRtrMldGrpIfSapMaxGroups, the maximum number of groups supported on the SAP. |
| Effect | N/A |
| Recovery | N/A |

43.3 vRtrMldGrpIfSapMaxGrpSrcLimExcd

Table 917: 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 vRtrMldGrplfSapMaxGrpSrcLimExcd 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 vRtrMldGrplfSapMaxGrpSources, the maximum number of group sources per group supported on the SAP. |
| Effect | N/A |
| Recovery | N/A |

43.4 vRtrMldGrplfSapMaxSrcsLimExceed

Table 918: vRtrMldGrplfSapMaxSrcsLimExceed properties

| Property name | Value |
|----------------------------------|---|
| Application name | MLD |
| Event ID | 2013 |
| Event name | vRtrMldGrplfSapMaxSrcsLimExceed |
| 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 \$vRtrMldGrplfSapMaxSources\$ for SAP |
| Cause | The vRtrMldGrplfSapMaxSrcsLimExceed 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 vRtrMldGrplfSapMaxSources, the maximum number of sources per group supported on the SAP. |
| Effect | N/A |
| Recovery | N/A |

43.5 vRtrMldGrplfSapMcacPlcyDropped

Table 919: vRtrMldGrplfSapMcacPlcyDropped properties

| Property name | Value |
|----------------------------------|--|
| Application name | MLD |
| Event ID | 2014 |
| Event name | vRtrMldGrplfSapMcacPlcyDropped |
| 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 vRtrMldGrplfSapMcacPlcyDropped 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 vRtrMldGrplfSapRxQueryVerMism

Table 920: vRtrMldGrplfSapRxQueryVerMism properties

| Property name | Value |
|----------------------------------|---|
| Application name | MLD |
| Event ID | 2016 |
| Event name | vRtrMldGrplfSapRxQueryVerMism |
| SNMP notification prefix and OID | TIMETRA-MLD-MIB.vRtrMldNotifications.16 |
| Default severity | warning |
| Source stream | main |
| Message format string | SAP configured for MLDv\$vRtrMldGrplfSapAdminVersion\$ received MLDv \$vRtrMldNotifyQueryVersion\$ query |
| Cause | A vRtrMldGrplfSapRxQueryVerMism 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 921: 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 <i>\$vRtrMldHostOperVersion\$</i> and query version <i>\$vRtrMldNotifyQueryVersion\$</i> |
| 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. vRtrMldHostAddress will identify the Host on which the query is received. vRtrMldHostOperVersion 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 922: 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 <i>\$vRtrMldNotifyDescription\$</i> |
| 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 923: 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 | <i>\$vRtrMldHostMaxGroups\$</i> exceeded on FwdSvdId <i>\$vRtrMldHostFwdSvcId\$</i> , GrpId <i>\$vRtrMldHostGrpId\$</i> |

| 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 vRtrMldHostMaxGroups, the maximum number of groups supported on the host. |
| Effect | N/A |
| Recovery | N/A |

43.10 vRtrMldHostMaxGrpSrcsLimitExcd

Table 924: 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 <i>\$vRtrMldHostMaxGrpSources\$</i> exceeded on Grp Ifld <i>\$vRtrMldHostGrpIfld\$</i> with FwdSvclid <i>\$vRtrMldHostFwdSvclid\$</i> |
| 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 925: 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 <i>\$vRtrMldHostMaxSources\$</i> exceeded on GrpIfId <i>\$vRtrMldHostGrpIfId\$</i> with FwdSvcId <i>\$vRtrMldHostFwdSvcId\$</i> |
| 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 926: 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 <i>\$vRtrMldNotifyGrpAddr\$</i> dropped on host <i>\$vRtrMldHostSubscriberId\$</i> after applying policy <i>\$vRtrMldNotifyMcacPolicyName\$</i> |

| 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 927: 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 Grplf |
| 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 928: 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 <i>\$vRtrMldHostAdminVersion\$</i> received query version <i>\$vRtrMldNotifyQueryVersion\$</i> |
| Cause | A vRtrMldHostRxQueryVerMismatch notification is generated when the MLD host is configured as MLDv2 but receives a MLDv1 Query. vRtrMldHostAddress will identify the Host on which the query is received. vRtrMldHostAdminVersion 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 929: 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 <i>\$vRtrIfIndex\$</i> compatible mode(<i>\$vRtrMldIfOperVersion\$</i>) and the version of the MLD query (version <i>\$vRtrMldNotifyQueryVersion\$</i>) 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 930: 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\$ <i>vRtrMldNotifyQueryVersion</i> \$ query received on interface \$ <i>vRtrIfIndex</i> \$ configured as MLDv\$ <i>vRtrMldIfAdminVersion</i> \$ |
| 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 931: 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 <i>\$ifName\$</i> has exceeded the maximum limit of <i>\$vRtrMldIfMaxGroups\$</i> |
| 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 932: 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 <i>\$vRtrMldIfMaxGrpSources\$</i> 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 933: 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 <i>\$vRtrMldIfMaxSources\$</i> 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 934: 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 <i>\$vRtrMldNotifyGrpAddr\$</i> dropped after applying <i>\$vRtrMldIfMcacPolicyName\$</i> |
| 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 935: 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 <i>\$vRtrMldNotifyGrpAddr\$/\$vRtrMldNotifySrcAddr\$</i> dropped for SLA profile instance subscriber <i>\$tmnxSubIdent\$</i> SAP <i>\$sapNotifyEncapValue\$</i> SLA profile <i>\$tmnxSubNotifSLAProfName\$</i> group <i>\$tmnxSubNotifSpiGroupID\$</i> due to of MCAC policy <i>\$vRtrMldNotifyMcacPolicyName\$</i> instance <i>\$vRtrID\$</i> , reason <i>\$vRtrMldNotifyDescription\$</i> |
| 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 vRtrMldNotifyMcacPolicyName. |
| 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 936: 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 <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> has exceeded the maximum limit of <i>\$sapMldSnpgCfgMaxNbrGrps\$</i> - Dropping group <i>\$tmnxMldSnpgGroupAddress\$</i> |
| 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 937: 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 <i>\$tmnxMldSnpgGroupAddress\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> could not be synced to MCS - <i>\$tmnxMldSnpgMcsFailureReason\$</i> |
| 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 938: *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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> has exceeded the maximum limit of <i>\$sdpBndMldSnpgCfgMaxNbrGrps\$</i> - Dropping group <i>\$tmnxMldSnpgGroupAddress\$</i> |
| 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 939: 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 <i>\$mplsTunnelName\$</i> 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 940: 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 <i>\$mplsTunnelName\$</i> 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 941: *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 <i>\$mplsTunnelName\$</i> 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 942: 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 <i>\$mplsTunnelName\$</i> 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 943: 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 <i>\$mplsXCName\$</i> 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 944: 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 <i>\$mplsXCName\$</i> 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 945: *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 <i>\$tmnxNotifyMplsResourceType\$</i> 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 946: *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 <i>\$tmnxNotifyMplsResourceType\$</i> resources has reached or exceeded <i>\$tmnxNotifyMplsResourceUsagePct\$%</i> 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 tmnxNotifyMplsResourceUsagePct. |
| Effect | The specified resource has reached or exceeded the warning threshold. |
| Recovery | There is no recovery required for this notification. |

45.9 tmnxMplsResourceRecovered

Table 947: 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 <i>\$tmnxNotifyMplsResourceType\$</i> resources has dropped below <i>\$tmnxNotifyMplsResourceUsagePct\$</i> % threshold. |
| Cause | The tmnxMplsResourceRecovered notification is generated when the usage of the resource specified by tmnxNotifyMplsResourceType drops below the warning threshold specified by tmnxNotifyMplsResourceUsagePct. This trap is generated only if the tmnxMplsResourceHighUsage 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 948: 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 <i>\$vRtrIfIndex\$</i> is in administrative state: <i>\$vRtrMplsIfAdminState\$</i> , IPv6 operational state: <i>\$vRtrMplsIfV6OperState\$</i> |
| 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 949: 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 <i>\$vRtrIfIndex\$</i> is in administrative state: <i>\$vRtrMplsIfAdminState\$</i> , operational state: <i>\$vRtrMplsIfOperState\$</i> |
| Cause | The MPLS interface changed state. |
| Effect | Service is affected. |
| Recovery | No recovery is required. |

45.12 vRtrMplsIPv6StateChange

Table 950: 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: <i>\$vRtrMplsGeneralAdminState\$</i> , IPv6 operational state: <i>\$vRtrMplsGeneralV6OperState\$</i> |
| 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 951: 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 | <p>Possible messages:</p> <ul style="list-style-type: none"> LSP <i>\$lspName\$</i> active path <i>\$lspOldPathName\$</i> has changed to active path <i>\$lspPathName\$</i> LSP <i>\$lspName\$</i> active path <i>\$lspOldPathName\$</i> has changed to active path <i>\$lspPathName\$</i> by manual method <i>\$vRtrMplsLspPathActiveByManual\$</i> |
| Cause | The vRtrMplsLspActivePathChanged notification is generated when the active path of an LSP successfully switches to a 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 vRtrMplsLspPathState 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 952: 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 <i>\$lspName\$</i> is operationally disabled ('shutdown') because <i>\$vRtrMplsLspNotificationReasonCode\$</i> |
| 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 953: 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 <i>\$lspName\$</i> failed because <i>\$vRtrMplsLspManualSwFailReason\$</i> |
| 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 vRtrMplsLspManualSwFailReason. |
| 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 954: 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 <i>\$lspPathName\$</i> is operationally disabled ('shutdown') because <i>\$vRtrMplsLspPathNotificationReasonCode\$</i> |
| 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 955: 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 <i>\$lspPathName\$</i> is <i>\$trapStatus\$</i> . <i>\$bandwidthChange\$</i> |

| 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 956: 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 957: 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 | <i>\$vRtrMplsLspPathLastMBBType\$</i> MBB <i>\$vRtrMplsLspPathMbbStatus\$</i> for LSP path <i>\$lspPathName\$</i> - reason <i>\$vRtrMplsLspPathMbbReasonCode\$</i> |
| 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 958: 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 <i>\$lspPathName\$</i> rerouted |
| Cause | An LSP Path has been rerouted. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

45.21 vRtrMplsLspPathResigned

Table 959: vRtrMplsLspPathResigned properties

| Property name | Value |
|----------------------------------|---|
| Application name | MPLS |
| Event ID | 2014 |
| Event name | vRtrMplsLspPathResigned |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.8 |
| Default severity | warning |
| Source stream | main |
| Message format string | LSP path <i>\$LspPathName\$</i> resigned as a result of <i>\$vRtrMplsLspPathLastMBBType\$</i> MBB |
| Cause | An LSP Path has resigned. |
| Effect | N/A |
| Recovery | N/A |

45.22 vRtrMplsLspPathSoftPreempted

Table 960: 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 <i>\$/spPathName\$</i> preempted |
| Cause | The vRtrMplsLspPathSoftPreempted notification is generated when an LSP Path is preempted. |
| Effect | N/A |
| Recovery | N/A |

45.23 vRtrMplsLspPathUp

Table 961: 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 <i>\$/spPathName\$</i> 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 962: 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 vRtrMplsResourceType 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 963: 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 <i>\$vRtrMplsLspSwitchStbyPathIndex\$</i> for lsp <i>\$lspName\$</i> failed because <i>\$vRtrMplsLspSwitchStbyReasonCode\$</i> |
| 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 964: 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 <i>\$lspName\$</i> 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 vRtrMplsNodeInlgpOverload

Table 965: 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 <i>\$vRtrMplsIgpOverloadIgpType\$</i> is in overload on router <i>\$vRtrMplsIgpOverloadRtrAddr\$</i> . |
| 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 966: 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 <i>\$vRtrMplsIgpOverloadIgpType\$</i> is in overload on router <i>\$vRtrMplsIgpOverloadRtrAddr\$</i> . |

| 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 vRtrMplsP2mplInstanceDown

Table 967: vRtrMplsP2mplInstanceDown properties

| Property name | Value |
|----------------------------------|--|
| Application name | MPLS |
| Event ID | 2016 |
| Event name | vRtrMplsP2mplInstanceDown |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.10 |
| Default severity | warning |
| Source stream | main |
| Message format string | P2MP instance <i>\$insName\$</i> LSP <i>\$lspName\$</i> is operationally disabled ('shutdown') because <i>\$vRtrMplsP2mplInstNotifReasonCode\$</i> |
| 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 vRtrMplsP2mplInstanceResignaled

Table 968: vRtrMplsP2mplInstanceResignaled properties

| Property name | Value |
|------------------|-------|
| Application name | MPLS |

| Property name | Value |
|----------------------------------|--|
| Event ID | 2023 |
| Event name | vRtrMplsP2mplInstanceResigned |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.17 |
| Default severity | warning |
| Source stream | main |
| Message format string | P2MP instance <i>\$insName\$</i> LSP <i>\$lspName\$</i> has been resigned as a result of <i>\$vRtrMplsP2mplInstLastMBBType\$</i> MBB |
| Cause | A P2MP instance was resigned. |
| Effect | Service is affected. |
| Recovery | No recovery is required. |

45.31 vRtrMplsP2mplInstanceUp

Table 969: vRtrMplsP2mplInstanceUp properties

| Property name | Value |
|----------------------------------|--|
| Application name | MPLS |
| Event ID | 2015 |
| Event name | vRtrMplsP2mplInstanceUp |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.9 |
| Default severity | warning |
| Source stream | main |
| Message format string | P2MP instance <i>\$insName\$</i> LSP <i>\$lspName\$</i> 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 970: 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 vRtrMplsS2ISubLspDown

Table 971: vRtrMplsS2ISubLspDown properties

| Property name | Value |
|----------------------------------|--|
| Application name | MPLS |
| Event ID | 2018 |
| Event name | vRtrMplsS2ISubLspDown |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.12 |
| Default severity | warning |
| Source stream | main |
| Message format string | S2L path <i>\$s2IName\$</i> to <i>\$vRtrMplsS2ISubLspNtDstAddr\$</i> for P2MP instance <i>\$insName\$</i> LSP <i>\$lspName\$</i> is operationally disabled ('shutdown') because <i>\$vRtrMplsS2ISubLspFailCode\$</i> |

| 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 vRtrMplsS2ISubLspPreempted

Table 972: vRtrMplsS2ISubLspPreempted properties

| Property name | Value |
|----------------------------------|---|
| Application name | MPLS |
| Event ID | 2036 |
| Event name | vRtrMplsS2ISubLspPreempted |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.30 |
| Default severity | minor |
| Source stream | main |
| Message format string | S2L path <i>\$s2IName\$</i> to <i>\$vRtrMplsS2ISubLspNtDstAddr\$</i> for P2MP instance <i>\$insName\$</i> for LSP <i>\$lspName\$</i> preempted |
| Cause | The vRtrMplsS2ISubLspPreempted notification is generated when an S2I sub LSP is soft-preempted. |
| Effect | If applicable, soft-preemption MBB will be started to resignal the S2I sub LSP. If the S2I sub LSP has not been resignaled by the time the preemption timer expires, the S2I will be torn down. |
| Recovery | There is no recovery required for this notification. |

45.35 vRtrMplsS2ISubLspRerouted

Table 973: vRtrMplsS2ISubLspRerouted properties

| Property name | Value |
|------------------|-------|
| Application name | MPLS |

| Property name | Value |
|----------------------------------|---|
| Event ID | 2019 |
| Event name | vRtrMplsS2ISubLspRerouted |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.13 |
| Default severity | warning |
| Source stream | main |
| Message format string | S2L path <i>\$s2IName\$</i> to <i>\$vRtrMplsS2ISubLspNtDstAddr\$</i> for P2MP instance <i>\$insName\$</i> for LSP <i>\$lspName\$</i> rerouted |
| Cause | An S2L Path was rerouted. |
| Effect | N/A |
| Recovery | N/A |

45.36 vRtrMplsS2ISubLspResigned

Table 974: vRtrMplsS2ISubLspResigned properties

| Property name | Value |
|----------------------------------|--|
| Application name | MPLS |
| Event ID | 2020 |
| Event name | vRtrMplsS2ISubLspResigned |
| SNMP notification prefix and OID | TIMETRA-MPLS-MIB.tmnxMplsNotifications.14 |
| Default severity | warning |
| Source stream | main |
| Message format string | S2L path <i>\$s2IName\$</i> to <i>\$vRtrMplsS2ISubLspNtDstAddr\$</i> for P2MP instance <i>\$insName\$</i> LSP <i>\$lspName\$</i> resigned as a result of <i>\$vRtrMplsS2ISubLspLastMBBType\$</i> MBB |
| Cause | An S2L Path was resigned. |
| Effect | N/A |
| Recovery | N/A |

45.37 vRtrMplsS2lSubLspUp

Table 975: 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 <i>\$s2lName\$</i> to <i>\$vRtrMplsS2lSubLspNtDstAddr\$</i> for P2MP instance <i>\$insName\$</i> LSP <i>\$lspName\$</i> 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 976: 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: <i>\$vRtrMplsGeneralAdminState\$</i> , operational state: <i>\$vRtrMplsGeneralOperState\$</i> |
| Cause | The MPLS module changed state. |
| Effect | Service is affected. |
| Recovery | No recovery is required. |

45.39 vRtrMplsXCBundleChange

Table 977: 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 | <i>\$vRtrMplsXCNotifyRednNumOfBitsSet\$</i> RSVP sessions <i>\$vRtrMplsXCNotifyRednBundlingType\$</i> starting from session number <i>\$vRtrMplsXCNotifyRednStartIndex\$</i> to <i>\$vRtrMplsXCNotifyRednEndIndex\$</i> |
| 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 978: 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 <i>\$TpLspName\$</i> switched from <i>\$vRtrMplsTpLspOldPathIndex \$</i> to <i>\$vRtrMplsTpLspPathIndex\$</i> 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 979: 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 <i>\$TpLspName\$</i> active on <i>\$vRtrMplsTpLspPathIndex\$</i> 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 980: 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 <i>\$vRtrMplsLspIndex\$</i> experiencing protection type mismatch: Rx 0x <i>\$vRtrMplsTpLspPtPathMepRxPdu\$</i> Tx 0x <i>\$vRtrMplsTpLspPtPathMepTxPdu\$</i> |
| 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 981: 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 982: 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 <i>\$vRtrMplsLspIndex\$</i> experiencing revertive mode mismatch: Rx 0x <i>\$vRtrMplsTpLspPtPathMepRxPdu\$</i> Tx 0x <i>\$vRtrMplsTpLspPtPathMepTxPdu\$</i> |
| 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 983: 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 <i>\$vRtrMplsLspIndex\$</i> experiencing revertive mode mismatch cleared: Rx 0x <i>\$vRtrMplsTpLspPtPathMepRxPdu\$</i> Tx 0x <i>\$vRtrMplsTpLspPtPathMepTxPdu\$</i> |
| 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 984: *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 <i>\$strPeer\$</i> 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 985: *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 <i>\$strPeer\$</i> has entered ESTABLISHED state. |
| Cause | The MSDP FSM entered the ESTABLISHED state. |
| Effect | N/A |
| Recovery | N/A |

47.3 tmnxMsdpNgActSrcLimExcd

Table 986: *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 <i>\$tmnxMsdpNgMaxActiveSources\$</i> has been exceeded.Num exceeded <i>\$tmnxMsdpNgStatusActSrcLimExceeded\$</i> . |
| 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 987: *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 <i>\$tmnxMsdpNgPeerGroupMaxActSources\$</i> reached for group <i>\$strGrpPref\$</i> . Num exceeded <i>\$tmnxMsdpNgPeerGroupActMsgsExMax\$</i> |
| 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 988: *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 <i>\$strLimit\$</i> for peer <i>\$strPeer\$</i> has been exceeded.Num exceeded <i>\$tmnxMsdpNgPeerStatsActSrcLimExcd\$</i> . |

| 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 989: 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 990: 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 <i>\$tmnxMsdpNgSourceMaxActiveSources\$</i> reached for source <i>\$strSrcPref\$</i> . Num exceeded <i>\$tmnxMsdpNgSourceSrcActMsgsExMax\$</i> |
| 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 991: *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 <i>\$tmnxNatDetAddrMapInStart\$</i> to <i>\$tmnxNatDetAddrMapInEnd\$</i> type <i>\$tmnxNatDetAddrMapSubType\$</i> nat-policy ' <i>\$tmnxNatDetAddrMapNatPolicy\$</i> ' changed to <i>\$tmnxNatDetAddrMapOperState\$</i> - <i>\$tmnxNatNotifyDescription\$</i> |
| Cause | The cause is explained in the <i>tmnxNatNotifyDescription</i> . |
| 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 992: *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 <i>\$tmnxNatDetPfxMapAddr/\$tmnxNatDetPfxMapAddrPrefixLength\$</i> type <i>\$tmnxNatDetPfxMapSubType\$</i> nat-policy ' <i>\$tmnxNatDetPfxMapNatPolicy\$</i> ' start <i>\$tmnxNatDetMap2InStart\$</i> end <i>\$tmnxNatDetMap2InEnd\$</i> changed to <i>\$tmnxNatDetMap2OperState\$</i> - <i>\$tmnxNatNotifyDescription\$</i> |
| 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 993: 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 <i>\$tmnxNatDetPfxMapAddr/\$tmnxNatDetPfxMapAddrPrefixLength\$</i> type <i>\$tmnxNatDetPfxMapSubType\$</i> nat-policy ' <i>\$tmnxNatDetPfxMapNatPolicy\$</i> ' changed to <i>\$tmnxNatDetPfxMapOperState\$</i> - <i>\$tmnxNatNotifyDescription\$</i> |
| 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 994: *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 tmnxNatDetPlcyTable 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 995: *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 <i>\$tmnxNatNotifyInsideAddr\$</i> / <i>\$tmnxNatNotifyInsideAddrPrefixLen\$</i> imported from the outside router instance <i>\$tmnxNatNotifyOutsideVRtrID\$</i> and associated with the NAT policy <i>\$tmnxNatNotifyName\$</i> in the inside router instance <i>\$tmnxNatNotifyInsideVRtrID\$</i> : <i>\$tmnxNatNotifyDescription\$</i> |
| Cause | The cause is explained in the <i>tmnxNatNotifyDescription</i> . |
| Effect | The destination-prefix is not imported. |
| Recovery | The recovery action logically follows from the specified cause. |

48.6 tmnxNatFwd2EntryAdded

Table 996: *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 | { <i>\$tmnxNatNotifyPISeqNum\$</i> } <i>\$tmnxNatNotifyTruthValue\$</i> <i>\$tmnxNatFwd2OutAddr\$</i> [<i>\$tmnxNatFwd2OutPort\$</i>] -- subscriber type <type> {<inside router> <inside IP> [AFTR <i>\$tmnxNatFwd2LsnAftrAddr\$</i>] <subscriber id> } <inside port> <protocol> from <i>\$tmnxNatFwd2Origin\$</i> |
| Cause | The <i>tmnxNatFwd2EntryAdded</i> notification is sent when a row is added to or removed from the <i>tmnxNatFwd2Table</i> ; 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 997: 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 \$tmnxNatFwd2NatPolicy\$ 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 998: 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 | <p>Possible messages:</p> <ul style="list-style-type: none"> • <code>{tmnxNatNotifyPISeqNum\$}</code> all blocks freed of all subscribers type <code>\$tmnxNatNotifySubscriberType\$</code> in inside router instance <code>\$tmnxNatNotifyInsideVRtrID\$</code> address type <code>\$tmnxNatNotifyInsideAddrType\$</code> prefix <code>\$tmnxNatNotifyInsideAddr\$/\$tmnxNatNotifyInsideAddrPrefixLen\$</code> MDA <code>\$tmnxNatNotifyMdaCardSlotNum\$/\$tmnxNatNotifyMdaSlotNum\$</code> ESA-VM <code>\$tmnxNatNotifyIlsaMemberEsaNum\$/\$tmnxNatNotifyIlsaMemberEsaVappNum\$</code> at <code>\$tmnxNatNotifyDateAndTime\$ - \$tmnxNatNotifyDescription\$</code> • <code>{tmnxNatNotifyPISeqNum\$}</code> all blocks freed of all subscribers type <code>\$tmnxNatNotifySubscriberType\$</code> with NAT policy index <code>\$tmnxNatNotifyPolicyIndex\$</code> in inside router instance <code>\$tmnxNatNotifyInsideVRtrID\$</code> address type <code>\$tmnxNatNotifyInsideAddrType\$</code> prefix <code>\$tmnxNatNotifyInsideAddr\$/\$tmnxNatNotifyInsideAddrPrefixLen\$</code> MDA <code>\$tmnxNatNotifyMdaCardSlotNum\$/\$tmnxNatNotifyMdaSlotNum\$</code> ESA-VM <code>\$tmnxNatNotifyIlsaMemberEsaNum\$/\$tmnxNatNotifyIlsaMemberEsaVappNum\$</code> at <code>\$tmnxNatNotifyDateAndTime\$ - \$tmnxNatNotifyDescription\$</code> |
| Cause | <p>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</p> |

| Property name | Value |
|---------------|--|
| | type. The values of <code>tmnxNatNotifyMdaChassisIndex</code> , <code>tmnxNatNotifyMdaCardSlotNum</code> and <code>tmnxNatNotifyMdaSlotNum</code> identify the ISA MDA where the blocks were processed. All notifications of this type are sequentially numbered with the <code>tmnxNatNotifyPISeqNum</code> . The value of <code>tmnxNatNotifyPolicyIndex</code> is the numerical identifier of the NAT policy used for this allocation; it can be used for correlation with the <code>tmnxNatPIBlockAllocationLsn</code> notification; the value zero means that this notification can be correlated with all the <code>tmnxNatPIBlockAllocationLsn</code> 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 <code>tmnxNatNotifyDescription</code> . |
| Effect | N/A |
| Recovery | N/A |

48.9 tmnxNatlsaGrplsDegraded

Table 999: *tmnxNatlsaGrplsDegraded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | NAT |
| Event ID | 2025 |
| Event name | <code>tmnxNatlsaGrplsDegraded</code> |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB.tmnxNatNotifications.25 |
| Default severity | minor |
| Source stream | main |
| Message format string | The NAT group <i>\$tmnxNatlsaGrpld\$</i> is <i>\$tmnxNatlsaGrpDegraded\$</i> . |
| Cause | The <code>tmnxNatlsaGrplsDegraded</code> notification is sent when the value of the object <code>tmnxNatlsaGrpDegraded</code> changes. |
| Effect | N/A |
| Recovery | N/A |

48.10 tmnxNatlsaGrpOperStateChanged

Table 1000: tmnxNatlsaGrpOperStateChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2024 |
| Event name | tmnxNatlsaGrpOperStateChanged |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB.tmnxNatNotifications.24 |
| Default severity | minor |
| Source stream | main |
| Message format string | The state of NAT group <i>\$tmnxNatlsaGrpId\$</i> changed to <i>\$tmnxNatlsaGrpOperState\$</i> . |
| Cause | The tmnxNatlsaGrpOperStateChanged notification is sent when the value of the object tmnxNatlsaGrpOperState changes. |
| Effect | N/A |
| Recovery | N/A |

48.11 tmnxNatlsaMemberSessionUsageHigh

Table 1001: tmnxNatlsaMemberSessionUsageHigh properties

| Property name | Value |
|----------------------------------|--|
| Application name | NAT |
| Event ID | 2002 |
| Event name | tmnxNatlsaMemberSessionUsageHigh |
| 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 <i>\$tmnxNatlsaMemberSessionUsageHi\$</i> . (EsaNum <i>\$tmnxNatlsaMemberEsaNum\$</i> , EsaVappNum <i>\$tmnxNatlsaMemberEsaVappNum\$</i>) |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.12 tmnxNatL2AwSublcmpPortUsageHigh

Table 1002: *tmnxNatL2AwSublcmpPortUsageHigh* properties

| Property name | Value |
|----------------------------------|--|
| Application name | NAT |
| Event ID | 2007 |
| Event name | tmnxNatL2AwSublcmpPortUsageHigh |
| 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 <i>\$tmnxNatL2AwSubStatlcmpPortUsageH\$</i> for subscriber <i>\$tmnxSubInfoSubIdent\$</i> using policy <i>\$tmnxNatL2AwSubStatNatPolicy\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.13 tmnxNatL2AwSubSessionUsageHigh

Table 1003: *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 <i>\$tmnxNatL2AwSubStatSessionUsageHi\$</i> for subscriber <i>\$tmnxSubInfoSubIdent\$</i> using policy <i>\$tmnxNatL2AwSubStatNatPolicy\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.14 tmnxNatL2AwSubTcpPortUsageHigh

Table 1004: *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 <i>\$tmnxNatL2AwSubStatTcpPortUsageHi\$</i> for subscriber <i>\$tmnxSubInfoSubIdent\$</i> using policy <i>\$tmnxNatL2AwSubStatNatPolicy\$</i> |
| Cause | N/A |

| Property name | Value |
|---------------|-------|
| Effect | N/A |
| Recovery | N/A |

48.15 tmnxNatL2AwSubUdpPortUsageHigh

Table 1005: 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 <i>\$tmnxNatL2AwSubStatUdpPortUsageHi\$</i> for subscriber <i>\$tmnxSubInfoSubIdent\$</i> using policy <i>\$tmnxNatL2AwSubStatNatPolicy\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.16 tmnxNatLsnSubBlksFree

Table 1006: 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 | { <i>\$tmnxNatNotifyPISeqNum\$</i> } LSN subscriber all blocks freed <i>\$tmnxNatNotifyLsnSubId\$ \$tmnxNatNotifySubscriberType\$ %\$tmnxNatNotifyNumber\$ \$tmnxNatNotifyInsideVRtrID\$ \$tmnxNatNotifyInsideAddr\$ MDA \$tmnxNatNotifyMdaCardSlotNum\$/\$tmnxNatNotifyMdaSlotNum\$ ESA-VM \$tmnxNatNotifyIsaMemberEsaNum\$/\$tmnxNatNotifyIsaMemberEsaVappNum\$</i> at <i>\$tmnxNatNotifyDateAndTime\$</i> |
| 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 tmnxNatNotifyPISeqNum. |
| Effect | N/A |
| Recovery | N/A |

48.17 tmnxNatLsnSublcmpPortUsgHigh

Table 1007: tmnxNatLsnSublcmpPortUsgHigh properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2026 |
| Event name | tmnxNatLsnSublcmpPortUsgHigh |
| 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 <i>\$tmnxNatQryLsnSubResIcmpPortUsgHi\$</i> for host <i>\$tmnxNatNotifyInsideAddr\$</i> in router <i>\$tmnxNatNotifyInsideVRtrID\$</i> 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 1008: 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 <i>\$tmnxNatQryLsnSubResSessionUsgHi\$</i> for host <i>\$tmnxNatNotifyInsideAddr\$</i> in router <i>\$tmnxNatNotifyInsideVRtrID\$</i> 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 1009: 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 <i>\$tmnxNatQryLsnSub ResTcpPortUsgHi\$</i> for host <i>\$tmnxNatNotifyInsideAddr\$</i> in router <i>\$tmnx NatNotifyInsideVRtrID\$</i> 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 1010: 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 <i>\$tmnxNatQryLsn SubResUdpPortUsgHi\$</i> for host <i>\$tmnxNatNotifyInsideAddr\$</i> in router <i>\$tmnxNatNotifyInsideVRtrID\$</i> 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 1011: 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 <i>\$tmnxNatMapDomName\$</i> mapping-rule <i>\$tmnxNatMapRuleName\$</i> rule-prefix= <i>\$tmnxNatMapRulePrefix\$</i> / <i>\$tmnxNatMapRulePrefixLength\$</i> ipv4-prefix= <i>\$tmnxNatMapRuleIpv4Prefix\$</i> / <i>\$tmnxNatMapRuleIpv4PrefixLength\$</i> ea-length= <i>\$tmnxNatMapRuleEaLength\$</i> |

| Property name | Value |
|---------------|--|
| | psid-offset= <i>\$tmnxNatMapRulePsidOffset\$</i> <i>\$tmnxNatNotifyTruthValue\$</i> in router <i>\$vRtrID\$</i> at <i>\$tmnxNatNotifyDateAndTime\$</i> |
| 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 1012: 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 <i>\$tmnxNatNotifyMemberSubOrHostDesc\$</i> on the group ISA member has been exceeded at <i>\$tmnxNatNotifyDateAndTime\$</i> . (group <i>\$tmnxNatNotifyIsaGrpId\$</i> - member <i>\$tmnxNatNotifyIsaMemberId\$</i> - chassis <i>\$tmnxNatNotifyMdaChassisIndex\$</i> - MDA <i>\$tmnxNatNotifyMdaCardSlotNum\$</i> / <i>\$tmnxNatNotifyMdaSlotNum\$</i> - ESA-VM <i>\$tmnxNatNotifyIsaMemberEsaNum\$</i> / <i>\$tmnxNatNotifyIsaMemberEsaVappNum\$</i>) |
| 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 1013: 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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxMDASlotNum\$</i> is now <i>\$tmnxNatNotifyTruthValue\$</i> in group <i>\$tmnxNatIsaGrpId\$</i> . |
| 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 1014: 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 <i>\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> in group <i>\$tmnxNatIlsaGrpId\$</i> has detected load sharing errors and has dropped <i>\$tmnxNatNotifyCounter\$</i> 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 1015: *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 <i>\$tmnxNatNotifyMemberSubOrHostDesc\$</i> on the group ISA member dropped below the threshold of 95% at <i>\$tmnxNatNotifyDateAndTime\$</i> . (group <i>\$tmnxNatNotifyIlsaGrpId\$</i> - member <i>\$tmnxNatNotifyIlsaMemberId\$</i> - chassis <i>\$tmnxNatNotifyMdaChassisIndex\$</i> - MDA <i>\$tmnxNatNotifyMdaCardSlotNum\$/\$tmnxNatNotifyMdaSlotNum\$</i> - ESA-VM <i>\$tmnxNatNotifyIlsaMemberEsaNum\$/\$tmnxNatNotifyIlsaMemberEsaVappNum\$</i>) |

| 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 1016: 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 <i>\$tmnxNatPcpSrvName\$</i> changed to <i>\$tmnxNatPcpSrvState\$</i> - <i>\$tmnxNatPcpSrvStateDescription\$</i> |
| 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 tmnxNatPIAddrFree

Table 1017: *tmnxNatPIAddrFree* properties

| Property name | Value |
|----------------------------------|--|
| Application name | NAT |
| Event ID | 2016 |
| Event name | tmnxNatPIAddrFree |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB.tmnxNatNotifications.16 |
| Default severity | minor |
| Source stream | main |
| Message format string | { <i>\$tmnxNatNotifyPISeqNum\$</i> } Free [<i>\$tmnxNatNotifyOutsideAddr\$ - \$tmnxNatNotifyOutsideEndAddr\$</i>] -- inside <i>\$insideVRtrIDName\$</i> at <i>\$tmnxNatNotifyDateAndTime\$ - \$tmnxNatNotifyDescription\$</i> |
| Cause | The <i>tmnxNatPIAddrFree</i> notification is sent when a range of outside IP addresses becomes free at once. The range starts at address <i>tmnxNatNotifyOutsideAddr</i> and ends with address <i>tmnxNatNotifyOutsideEndAddr</i> . It replaces a number of <i>tmnxNatPIBlockAllocationL2Aw</i> or <i>tmnxNatPIBlockAllocationLsn</i> 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 <i>tmnxNatNotifyDescription</i> . If the value of <i>tmnxNatNotifyInsideVRtrID</i> 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 <i>tmnxNatNotifyInsideVRtrID</i> is equal to zero, it means that all the port blocks are released. |
| Effect | N/A |
| Recovery | N/A |

48.28 *tmnxNatPIBlockAllocationL2Aw*

Table 1018: *tmnxNatPIBlockAllocationL2Aw* properties

| Property name | Value |
|------------------|------------------------------|
| Application name | NAT |
| Event ID | 2013 |
| Event name | tmnxNatPIBlockAllocationL2Aw |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-NAT-MIB.tmnxNatNotifications.13 |
| Default severity | minor |
| Source stream | main |
| Message format string | { <i>\$tmnxNatNotifyPISeqNum\$</i> } <i>\$tmnxNatNotifyTruthValue\$</i> <i>\$tmnxNatNotifyOutsideAddr\$</i> [<i>\$tmnxNatNotifyPort\$-\$tmnxNatNotifyPort2\$</i>] -- l2-aware-sub <i>\$tmnxNatNotifyL2AwSubIdent\$</i> policy <i>\$tmnxNatNotifyName\$</i> <i>\$tmnxNatNotifyInsideAddr\$</i> at <i>\$tmnxNatNotifyDateAndTime\$</i> |
| Cause | The tmnxNatPIBlockAllocationL2Aw 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 tmnxNatNotifyPort 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 tmnxNatPIBlockAllocationLsn

Table 1019: tmnxNatPIBlockAllocationLsn properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2012 |
| Event name | tmnxNatPIBlockAllocationLsn |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB.tmnxNatNotifications.12 |
| Default severity | minor |
| Source stream | main |
| Message format string | { <i>\$tmnxNatNotifyPISeqNum\$</i> } Map <i>\$tmnxNatNotifyTruthValue\$</i> <i>\$tmnxNatNotifyOutsideAddr\$</i> [<i>\$tmnxNatNotifyPort\$-\$tmnxNatNotifyPort2\$</i>] MDA <i>\$tmnxNatNotifyMdaCardSlotNum\$</i> / <i>\$tmnxNatNotifyMdaSlotNum\$</i> |

| Property name | Value |
|---------------|---|
| | <code>\$ ESA-VM \$tmnxNatNotifyIsaMemberEsaNum\$/\$tmnxNatNotifyIsaMemberEsaVappNum\$</code> |
| Cause | The <code>tmnxNatPIBlockAllocationLsn</code> 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 <code>tmnxNatNotifyOutsideVRtrID</code> and the outside IP address <code>tmnxNatNotifyOutsideAddr</code> ; it starts with port <code>tmnxNatNotifyPort</code> and ends with port <code>tmnxNatNotifyPort2</code> . The NAT subscriber is identified with its subscriber ID <code>tmnxNatNotifyLsnSubId</code> . To further facilitate the identification of the NAT subscriber, its type <code>tmnxNatNotifySubscriberType</code> , inside IP address <code>tmnxNatNotifyInsideAddr</code> and inside virtual router instance <code>tmnxNatNotifyInsideVRtrID</code> are provided. The values of <code>tmnxNatNotifyMdaChassisIndex</code> , <code>tmnxNatNotifyMdaCardSlotNum</code> and <code>tmnxNatNotifyMdaSlotNum</code> identify the ISA MDA where this block is processed. The value of <code>tmnxNatNotifyNumber</code> is the numerical identifier of the NAT policy used for this allocation; it can be used for correlation of notifications, especially with the <code>tmnxNatPIAddrFree</code> summary event, that may indicate this number in the <code>tmnxNatNotifyDescription</code> object. When the block allocation is made, the value of the object <code>tmnxNatNotifyTruthValue</code> is 'true'; when the block allocation expires, it is 'false'. |
| Effect | N/A |
| Recovery | N/A |

48.30 tmnxNatPIL2AwBlockUsageHigh

Table 1020: `tmnxNatPIL2AwBlockUsageHigh` properties

| Property name | Value |
|----------------------------------|--|
| Application name | NAT |
| Event ID | 2001 |
| Event name | <code>tmnxNatPIL2AwBlockUsageHigh</code> |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB. <code>tmnxNatNotifications.1</code> |
| Default severity | warning |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | The block usage high water status changed to <i>\$tmnxNatPIBlockUsageHi\$</i> . |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.31 tmnxNatPIL2AwMembrBlockUsageHigh

Table 1021: *tmnxNatPIL2AwMembrBlockUsageHigh* properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2044 |
| Event name | tmnxNatPIL2AwMembrBlockUsageHigh |
| 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 <i>\$tmnxNatPIL2AwSubscrUsageHi\$</i> for pool <i>\$tmnxNatPIName\$</i> on ISA group <i>\$tmnxNatIsaGrpId\$</i> member <i>\$tmnxNatIsaMemberId\$</i> MDA chassis <i>\$tmnxNatIsaMemberMdaChassisIndex\$</i> card slot <i>\$tmnxNatIsaMemberMdaCardSlotNum\$</i> slot <i>\$tmnxNatIsaMemberMdaSlotNum\$</i> ESA-VM <i>\$tmnxNatIsaMemberEsaNum\$</i> <i>\$tmnxNatIsaMemberEsaVappNum\$</i> |
| Cause | The tmnxNatPIL2AwMembrBlockUsageHigh 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 tmnxNatPILsnMemberBlockUsageHigh

Table 1022: tmnxNatPILsnMemberBlockUsageHigh properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2003 |
| Event name | tmnxNatPILsnMemberBlockUsageHigh |
| 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 <i>\$tmnxNatPILsnMemberBlockUsageHi\$</i> for pool <i>\$tmnxNatPILName\$</i> on ISA group <i>\$tmnxNatIsaGrpId\$</i> member <i>\$tmnxNatIsaMemberId\$</i> MDA <i>\$tmnxNatIsaMemberMdaCardSlotNum\$</i> / <i>\$tmnxNatIsaMemberMdaSlotNum\$</i> ESA-VM <i>\$tmnxNatIsaMemberEsaNum\$</i> / <i>\$tmnxNatIsaMemberEsaVappNum\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.33 tmnxNatPILsnMemberPortUsageHigh

Table 1023: tmnxNatPILsnMemberPortUsageHigh properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2046 |
| Event name | tmnxNatPILsnMemberPortUsageHigh |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB.tmnxNatNotifications.46 |
| Default severity | warning |

| Property name | Value |
|-----------------------|--|
| Source stream | main |
| Message format string | <p>Possible messages:</p> <ul style="list-style-type: none"> The port usage high water status changed to <i>\$tmnxNatNotifyPILsnMbrPortUsageHi\$</i> for router <i>\$vRtrID\$</i> pool <i>\$tmnxNatNotifyPoolName\$</i> protocol <i>\$tmnxNatNotifyPILsnMbrProtocol\$</i> on ISA group <i>\$tmnxNatIlsaGrpld\$</i> member <i>\$tmnxNatIlsaMemberId\$</i> MDA chassis <i>\$tmnxNatIlsaMemberMdaChassisIndex\$</i> card slot <i>\$tmnxNatIlsaMemberMdaCardSlotNum\$</i> slot <i>\$tmnxNatIlsaMemberMdaSlotNum\$</i> ESA-VM <i>\$tmnxNatIlsaMemberEsaNum\$</i>/<i>\$tmnxNatIlsaMemberEsaVappNum\$</i> The port usage high water status changed to <i>\$tmnxNatNotifyPILsnMbrPortUsageHi\$</i> for router <i>\$vRtrID\$</i> pool <i>\$tmnxNatNotifyPoolName\$</i> protocol <i>\$tmnxNatNotifyPILsnMbrProtocol\$</i> on ISA group <i>\$tmnxNatIlsaGrpld\$</i> member <i>\$tmnxNatIlsaMemberId\$</i> MDA chassis <i>\$tmnxNatIlsaMemberMdaChassisIndex\$</i> card slot <i>\$tmnxNatIlsaMemberMdaCardSlotNum\$</i> slot <i>\$tmnxNatIlsaMemberMdaSlotNum\$</i> ESA-VM <i>\$tmnxNatIlsaMemberEsaNum\$</i>/<i>\$tmnxNatIlsaMemberEsaVappNum\$</i> Outside address <i>\$tmnxNatNotifyOutsideAddr\$</i> |
| Cause | The tmnxNatPILsnMemberPortUsageHigh 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 tmnxNatPILsnRedActiveChanged

Table 1024: tmnxNatPILsnRedActiveChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2017 |
| Event name | tmnxNatPILsnRedActiveChanged |
| 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 <i>\$tmnxNatPILsnRedActive\$</i> for pool <i>\$tmnxNatPName\$ - \$tmnxNatNotifyDescription\$</i> |
| Cause | The <i>tmnxNatPILsnRedActiveChanged</i> notification is sent when the value of the object <i>tmnxNatPILsnRedActive</i> changes. The cause is explained in the <i>tmnxNatNotifyDescription</i> . |
| Effect | While the value of the object <i>tmnxNatPILsnRedActive</i> 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 <i>tmnxNatVrtrInRedSteerRt</i> is not advertised in the realm of any inside virtual router instance associated with this pool; - NAT traffic matching a filter with <i>TFilterAction</i> equal to 'nat' is redirected to the address specified with <i>tmnxNatVrtrInRedPeerAddr</i> or dropped if <i>tmnxNatVrtrInRedPeerAddr</i> 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 <i>tmnxNatPILsnRedExpPrefix</i> 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 <i>tmnxNatNotifyDescription</i> . |

48.35 tmnxNatPIMemberExtBlockUsageHigh

Table 1025: *tmnxNatPIMemberExtBlockUsageHigh* properties

| Property name | Value |
|----------------------------------|---|
| Application name | NAT |
| Event ID | 2045 |
| Event name | <i>tmnxNatPIMemberExtBlockUsageHigh</i> |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB. <i>tmnxNatNotifications.45</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | The extended port block usage high water status changed to <i>\$tmnxNatNotifyMbrExPrtBckUsageHi\$</i> for router <i>\$vRtrID\$</i> pool <i>\$tmnxNatNotifyPoolName\$</i> on ISA group <i>\$tmnxNatIsaGrpId\$</i> member <i>\$tmnx</i> |

| Property name | Value |
|---------------|---|
| | <i>NatIsaMemberId</i> \$ MDA chassis <i>\$tmnxNatIsaMemberMdaChassisIndex</i> \$ card slot <i>\$tmnxNatIsaMemberMdaCardSlotNum</i> \$ slot <i>\$tmnxNatIsaMemberMdaSlotNum</i> \$ ESA-VM <i>\$tmnxNatIsaMemberEsaNum</i> ! <i>\$tmnxNatIsaMemberEsaVappNum</i> \$ Outside address <i>\$tmnxNatNotifyOutsideIPv4Addr</i> \$ |
| Cause | The <i>tmnxNatPIMemberExtBlockUsageHigh</i> 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 1026: *tmnxNatResourceProblemCause* properties

| Property name | Value |
|----------------------------------|--|
| Application name | NAT |
| Event ID | 2015 |
| Event name | <i>tmnxNatResourceProblemCause</i> |
| SNMP notification prefix and OID | TIMETRA-NAT-MIB. <i>tmnxNatNotifications</i> .15 |
| Default severity | minor |
| Source stream | main |
| Message format string | <i>\$tmnxNatNotifyDescription</i> \$ |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.37 *tmnxNatResourceProblemDetected*

Table 1027: *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 <i>\$tmnxNatResourceProblem\$</i> . |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

48.38 tmnxNatVappActive

Table 1028: *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 <i>\$tmnxNatEsaNum\$/\$tmnxNatEsaVappNum\$</i> is now <i>\$tmnxNatNotifyTruthValue\$</i> in group <i>\$tmnxNatIsaGrpld\$</i> . |
| 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 1029: 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 <i>\$tmnxNatEsaNum\$</i> / <i>\$tmnxNatEsaVapp Num\$</i> in group <i>\$tmnxNatIsaGrpId\$</i> has detected load sharing errors and has dropped <i>\$tmnxNatNotifyCounter\$</i> 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 1030: *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 <i>\$tmnxNatNotify TruthValue\$</i> : <i>\$tmnxNatVrtrOutDnatOnlyRoutes\$</i> / <i>\$tmnxNatVrtrOutDnat OnlyRouteLimit\$</i> . |
| Cause | The <i>tmnxNatVrtrOutDnatOnlyRoutesHigh</i> notification is sent with the value 'true' for <i>tmnxNatNotifyTruthValue</i> when the actual value of the object <i>tmnxNatVrtrOutDnatOnlyRoutes</i> approaches the configured value of <i>tmnxNatVrtrOutDnatOnlyRouteLimit</i> for a given virtual router instance. The same notification is sent with 'false' for <i>tmnxNatNotify TruthValue</i> when the value of <i>tmnxNatVrtrOutDnatOnlyRoutes</i> goes below the threshold value again. |
| Effect | While the value of <i>tmnxNatVrtrOutDnatOnlyRoutes</i> is between the threshold value and the <i>tmnxNatVrtrOutDnatOnlyRouteLimit</i> 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 <i>tmnxNat VrtrOutDnatOnlyRoutes</i> would exceed the <i>tmnxNatVrtrOutDnatOnly RouteLimit</i> limit, the system would refuse that attempt. |
| Recovery | Within the associated NAT inside virtual router instance, - reduce the number of prefixes (in the <i>tmnxNatPrefixTable</i>), - reduce the value of <i>tmnxNatVrtrInMaxDetSubscrLimit</i> . |

49 NTP

49.1 tmnxNtpAuthMismatch

Table 1031: tmnxNtpAuthMismatch properties

| Property name | Value |
|----------------------------------|---|
| Application name | NTP |
| Event ID | 2001 |
| Event name | tmnxNtpAuthMismatch |
| SNMP notification prefix and OID | TIMETRA-NTP-MIB.tmxNtpNotifications.1 |
| Default severity | warning |
| Source stream | main |
| Message format string | NTP message is received with an <i>\$tmnxNtpAuthKeyFailType\$</i> from <i>\$tmnxNtpPeersPeerAddress\$</i> in <i>\$tmnxNtpPeersPeerVRtrID\$</i> |
| Cause | The tmnxNtpAuthMismatch notification is generated when tmnxNtpAuthCheck has a value of true and an NTP message is received with an incorrect authentication key, key id, or key type. tmnxNtpPeersPeerAddrType 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 1032: *tmnxNtpNoServersAvail* properties

| Property name | Value |
|----------------------------------|---------------------------------------|
| Application name | NTP |
| Event ID | 2002 |
| Event name | tmnxNtpNoServersAvail |
| SNMP notification prefix and OID | TIMETRA-NTP-MIB.tmxNtpNotifications.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 1033: *tmnxNtpOperChange* properties

| Property name | Value |
|----------------------------------|--|
| Application name | NTP |
| Event ID | 2008 |
| Event name | tmnxNtpOperChange |
| SNMP notification prefix and OID | TIMETRA-NTP-MIB.tmxNtpNotifications.7 |
| Default severity | warning |
| Source stream | main |
| Message format string | NTP's operational status is <i>\$tmnxNtpOperState\$</i> |
| Cause | There has been a change in the operational state of NTP. |
| Effect | N/A |
| Recovery | N/A |

49.4 tmnxNtpServerChange

Table 1034: 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 <i>\$strOldServer\$</i> in <i>\$intOldVRtrId\$</i> , New server <i>\$tmnxNtpPeersPeerAddress\$</i> in <i>\$tmnxNtpPeersPeerVRtrID\$</i> |
| 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 1035: 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 svcldInvalid

Table 1036: *svcldInvalid* properties

| Property name | Value |
|----------------------------------|---|
| Application name | OAM |
| Event ID | 2053 |
| Event name | svcldInvalid |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | main |
| Message format string | Service id <i>\$serviceId\$</i> is invalid: <i>\$reasonToReport\$</i> |
| Cause | Svc-ping tried to send or process a packet to a non-existent svc-id. |
| Effect | N/A |
| Recovery | N/A |

50.2 svcldWrongType

Table 1037: *svcldWrongType* properties

| Property name | Value |
|----------------------------------|----------------|
| Application name | OAM |
| Event ID | 2054 |
| Event name | svcldWrongType |
| SNMP notification prefix and OID | N/A |

| Property name | Value |
|-----------------------|---|
| Default severity | minor |
| Source stream | main |
| Message format string | Service id <i>\$serviceId\$</i> has a wrong type: <i>\$reasonToReport\$</i> |
| 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 1038: *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 <i>\$tmnxOamAncpHistoryAncpString\$</i> has ended. The access Node has sent Result <i>\$tmnxOamAncpHistoryAccNodeResult\$</i> ; code <i>\$tmnxOamAncpHistoryAccNodeCode\$</i> ; and reply string <i>\$tmnxOamAncpHistoryAccNodeRspStr\$</i> . |
| Cause | An ANCP loopback is finished and a notification was explicitly requested. |
| Effect | N/A |
| Recovery | N/A |

50.4 tmnxAncpLoopbackTestCompletedL

Table 1039: *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 <i>\$tmnxOamAncpHistoryAncpString\$</i> has ended. The access Node has sent Result <i>\$tmnxOamAncpHistoryAccNodeResult\$</i> ; code <i>\$tmnxOamAncpHistoryAccNodeCode\$</i> ; and reply string <i>\$tmnxOamAncpHistoryAccNodeRspStr\$</i> . |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

50.5 tmnxOamDiagTestCompleted

Table 1040: *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 <i>\$tmnxOamDiagCtlTestMode\$</i> test " <i>\$tmnxOamDiagCtlTestIndex\$</i> " created by " <i>\$tmnxOamDiagCtlOwnerIndex\$</i> " run # <i>\$tmnxOamTestRunIndex\$</i> completed |

| Property name | Value |
|---------------|--|
| Cause | A tmnxOamDiagTestCompleted trap is generated at the end of every diagnostic test run. A diagnostic test is configured using tmnxOamDiagCtlTable. 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 1041: 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 <i>\$tmnxOamLTtraceAutoDiscoveryState\$</i> |
| 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 1042: *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 <i>\$strTmnxOamLTtraceFecPrefix\$</i> / <i>\$strTmnxOamLTtraceFecPrefLen\$</i> is discovered with <i>\$tmnxOamLTtraceFecDisPaths\$</i> paths. The discovery status BITS are <i>\$strTmnxOamLTtraceFecDisStatusBits\$</i> . |
| 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 1043: *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, <i>\$strTmnxOamLTtraceFecPrefix\$</i> / <i>\$strTmnxOamLTtraceFecPrefLen\$</i> . <i>\$tmnx</i> |

| Property name | Value |
|---------------|---|
| | <i>OamLTtraceFecFailedProbes</i> out of <i>\$tmnxOamLTtraceFecDisPaths</i> 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 1044: *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, <i>\$strTmnxOamLTtraceFecPrefix</i> / <i>\$strTmnxOamLTtraceFecPrefLen</i> , has changed to <i>\$tmnxOamLTtraceFecProbeState</i> . <i>\$tmnxOamLTtraceFecFailedProbes</i> out of <i>\$tmnxOamLTtraceFecDisPaths</i> 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 1045: *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 #tmnxOamPingResultsTestRunIndex\$ probe \$tmnxOamPingHistoryIndex\$ failed |
| Cause | A probe failure was detected when the corresponding tmnxOamPingCtlTrapGeneration object is set to probeFailure(0) subject to the value of tmnxOamPingCtlTrapProbeFailureFilter. The object tmnxOamPingCtlTrapProbeFailureFilter 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 1046: *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 <i>\$tmnxOamPingCtlTestMode\$</i> test " <i>\$tmnxOamPingCtlTestIndex\$</i> " created by " <i>\$tmnxOamPingCtlOwnerIndex\$</i> " run # <i>\$tmnxOamPingResultsTestRunIndex\$</i> completed |
| Cause | A ping test when the corresponding <i>tmnxOamPingCtlTrapGeneration</i> object is set to <i>testCompletion(2)</i> . |
| Effect | N/A |
| Recovery | N/A |

50.12 *tmnxOamPingTestFailedV3*

Table 1047: *tmnxOamPingTestFailedV3* properties

| Property name | Value |
|----------------------------------|--|
| Application name | OAM |
| Event ID | 2002 |
| Event name | <i>tmnxOamPingTestFailedV3</i> |
| SNMP notification prefix and OID | TIMETRA-OAM-TEST-MIB. <i>tmnxOamPingNotifications.9</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | OAM <i>\$tmnxOamPingCtlTestMode\$</i> test " <i>\$tmnxOamPingCtlTestIndex\$</i> " created by " <i>\$tmnxOamPingCtlOwnerIndex\$</i> " run # <i>\$tmnxOamPingResultsTestRunIndex\$</i> failed |
| Cause | A ping test failed when the corresponding <i>tmnxOamPingCtlTrapGeneration</i> object is set to <i>testFailure(1)</i> . In this instance <i>tmnxOamPingCtlTrapTestFailureFilter</i> 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 1048: *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 " <i>\$tmnxOamPmCfgSessName\$</i> ", test type <i>\$tmnxOamPmStsBaseTestType\$</i> , measurement interval duration <i>\$tmnxOamPmStsMeasIntvlDuration\$</i> , MI start <i>\$tmnxOamPmStsBaseStartTime\$</i> UTC, delay bin type <i>\$tmnxOamPmNotifThrDelayBinType\$</i> . Threshold type <i>\$tmnxOamPmNotifThrType\$</i> , direction <i>\$tmnxOamPmNotifThrDirection\$</i> , bin lower bound (us) <i>\$tmnxOamPmNotifThrBinLowerBound\$</i> , configured threshold <i>\$tmnxOamPmNotifThrCfgClear\$</i> , operational value <i>\$tmnxOamPmNotifThrOperClear\$</i> . TCA type <i>\$tmnxOamPmNotifThrStateType\$</i> , suspect flag <i>\$tmnxOamPmStsBaseSuspect\$</i> . |
| Cause | A <i>tmnxOamPmThrClear</i> 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 <i>tmnxOamPmThrClear</i> trap is sent per <i>tmnxOamPmThrRaise</i> trap. OAM-PM thresholds are explained in the description clauses of <i>tmnxOamPmCfgThrDelay</i> Table, <i>tmnxOamPmCfgThrLossFwBwAg</i> Table, and <i>tmnxOamPmCfgThrLossFwBw</i> Table. OAM-PM counters are explained in the description clauses of the <i>tmnxOamPmStatsTableObjs</i> 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 1049: *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 " <i>\$tmnxOamPmCfgSessName\$</i> ", test type <i>\$tmnxOamPmStsBaseTestType\$</i> , measurement interval duration <i>\$tmnxOamPmStsMeasIntvlDuration\$</i> , MI start <i>\$tmnxOamPmStsBaseStartTime\$</i> UTC, delay bin type <i>\$tmnxOamPmNotifThrDelayBinType\$</i> . Threshold type <i>\$tmnxOamPmNotifThrType\$</i> , direction <i>\$tmnxOamPmNotifThrDirection\$</i> , bin lower bound (us) <i>\$tmnxOamPmNotifThrBinLowerBound\$</i> , configured threshold <i>\$tmnxOamPmNotifThrCfgRaise\$</i> , operational value <i>\$tmnxOamPmNotifThrOperRaise\$</i> . TCA type <i>\$tmnxOamPmNotifThrStateType\$</i> , suspect flag <i>\$tmnxOamPmStsBaseSuspect\$</i> . |
| Cause | A <i>tmnxOamPmThrRaise</i> 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. <i>tmnxOamPmCfgThrLossAvgFlrRaise</i>) is met or exceeded, the <i>tmnxOamPmThrRaise</i> trap is sent at the end of the measurement interval. If another type of threshold (e.g. <i>tmnxOamPmCfgThrLossHliRaise</i>) is met or exceeded, the <i>tmnxOamPmThrRaise</i> 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 <i>tmnxOamPmThrRaise</i> trap is sent per threshold type during one OAM-PM measurement interval. For example, at most one <i>tmnxOamPmThrRaise</i> 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 'oamPmSession1'. OAM-PM thresholds are explained in the description clauses of <i>tmnxOamPmCfgThrDelayTable</i> , <i>tmnxOamPmCfgThrLossFwBwAgTable</i> , and <i>tmnxOamPmCfgThrLossFwBwTable</i> . OAM-PM counters are explained in the description clauses of the <i>tmnxOamPmStatsTableObjs</i> 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 1050: 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 <i>\$tmnxOamSaaCtlTestMode\$</i> test " <i>\$tmnxOamSaaCtlTestIndex\$</i> " created by " <i>\$tmnxOamSaaCtlOwnerIndex\$</i> " run # <i>\$tmnxOamSaaTTestRunIndex\$</i> crossed <i>\$tmnxOamSaaTDirection\$</i> <i>\$tmnxOamSaaTType\$</i> threshold <i>\$tmnxOamSaaTThreshold\$</i> with value <i>\$tmnxOamSaaTValue\$</i> |
| 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 1051: 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 1052: 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 1053: 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 1054: 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 <i>\$tmnxOamTrCtlTestMode\$</i> test " <i>\$tmnxOamTrCtlTestIndex\$</i> " created by " <i>\$tmnxOamTrCtlOwnerIndex\$</i> " run # <i>\$tmnxOamTrResultsTestRunIndex\$</i> completed |
| Cause | The OAM trace route test has just completed. |
| Effect | N/A |
| Recovery | N/A |

50.20 tmnxOamTrTestFailed

Table 1055: *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 <i>\$tmnxOamTrCtlTestMode\$</i> test " <i>\$tmnxOamTrCtlTestIndex\$</i> " created by " <i>\$tmnxOamTrCtlOwnerIndex\$</i> " run # <i>\$tmnxOamTrResultsTestRunIndex\$</i> failed |
| Cause | The OAM trace route test failed to complete successfully. |
| Effect | N/A |
| Recovery | N/A |

50.21 tmnxTwampRflInactivityTimeout

Table 1056: *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 | <p>TWAMP Reflector test session localAddr <i>\$tmnxTwampRflNotifLocalAddr\$</i> port <i>\$tmnxTwampRflNotifLocalUdpPort\$</i> remoteAddr <i>\$tmnxTwampRflNotifRemoteAddr\$</i> port <i>\$tmnxTwampRflNotifRemoteUdpPort\$</i> disconnected because REFWAIT expired, Client Connection Addr <i>\$tmnxTwampSrvNotifClientAddr\$</i></p> |
| 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 1057: *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 <i>\$tmnxTwampSrvConnClientAddr\$</i> disconnected because it was inactive for <i>\$tmnxTwampSrvConnIdleTime\$</i> seconds |
| Cause | The <i>tmnxTwampSrvInactivityTimeout</i> 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 (<i>tmnxTwampSrvInactTimeout</i>). |
| 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 1058: *tmnxTwampSrvMaxConnsExceeded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | OAM |
| Event ID | 2201 |
| Event name | <i>tmnxTwampSrvMaxConnsExceeded</i> |
| SNMP notification prefix and OID | TIMETRA-TWAMP-MIB. <i>tmnxTwampNotifications.2</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | TWAMP server control connection to client <i>\$tmnxTwampSrvNotifClientAddr\$</i> could not be established because the system limit (<i>\$tmnxTwampSrvConnectionCount\$</i> concurrent connections) has been reached |
| Cause | The <i>tmnxTwampSrvMaxConnsExceeded</i> 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 (<i>tmnxTwampSrvMaxConnections</i>) 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 1059: 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 <i>\$tmnxTwampSrvNotifClientAddr\$</i> could not be established because the system limit (<i>\$tmnxTwampSrvSessionCount\$</i> 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 1060: 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 <i>\$tmnxTwampSrvNotifClientAddr\$</i> could not be established because the limit for prefix <i>\$tmnxTwampSrvPrefixAddr\$</i> / <i>\$tmnxTwampSrvPrefixLen\$</i> (<i>\$tmnxTwampSrvPfxConnCount\$</i> concurrent connections) has been reached |
| Cause | The <i>tmnxTwampSrvPfxMaxConnsExceeded</i> 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 (<i>tmnxTwampSrvPrefixMaxConnections</i>) 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 1061: *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 <i>\$tmnxTwampSrvNotifClientAddr\$</i> could not be established because the limit for prefix <i>\$tmnxTwampSrv</i> |

| Property name | Value |
|---------------|---|
| | <i>PrefixAddr</i> \$/ <i>\$tmnxTwampSrvPrefixLen</i> \$ (<i>\$tmnxTwampSrvPfxSessionCount</i> \$ concurrent sessions) has been reached |
| Cause | The <i>tmnxTwampSrvPfxMaxSessExceeded</i> 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 (<i>tmnxTwampSrvPrefixMaxSessions</i>) 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 1062: 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 " <i>\$tmnxOFSwitch Name\$</i> " flow-table <i>\$tmnxOFFlowTableId\$</i> . Flow-table Oper Status: <i>\$tmnxOFFlowTableOperStatus\$</i> . Failure Reason <i>\$tmnxOFNotify Description\$</i> |
| 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)'. 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 1063: 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 1064: 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 \$ospfLsdbRtrId\$ |
| 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 1065: 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 \$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 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 1066: 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 1067: 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 1068: 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 1069: *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 <i>\$tmnxOspfHostnameName\$</i> |
| 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 1070: *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 <i>\$tmnxOspfExportLimit\$</i> , 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 1071: 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 <i>\$tmnxOspfExportLimitLogPercent\$</i> percent of the export limit <i>\$tmnxOspfExportLimit\$</i> |
| 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 1072: 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 <i>\$tmnxOspfRouterId\$</i> : OSPF disabled. Reason: <i>\$tmnxOspfFailureReasonCode\$</i> |
| 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 1073: 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 <i>\$tmnxOspfFlexAlgoId\$</i> in area <i>\$tmnxOspfAreaId\$</i> is operationally down due to <i>\$tmnxOspfNotifyDescription\$</i> . |
| 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 1074: 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 1075: 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 <i>\$ospfRouterIdIpAddr\$</i> : Number of external LSAs has exceeded the configured limit (<i>\$tmnxOspfExtLsdbLimit\$</i>) |
| 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 1076: *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 <i>\$ospfRouterIdIpAddr\$</i> : Packet failed <i>\$tmnxOspfConfigErrorType\$</i> authentication on interface <i>\$ospfIfIpAddress\$</i> from <i>\$tmnxOspfPacketSrcAddress\$</i> in <i>\$tmnxOspfPacketType\$</i> |
| 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 1077: 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 1078: 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 1079: 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 \$tmnxOspfIfName\$ 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 1080: 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 <i>\$vRtrIfIndex\$</i> because <i>\$strReason\$</i> . |
| 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 1081: 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 <i>\$vRtrIfIndex\$</i> . |
| 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 1082: *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 <i>\$ospfRouterIdIpAddr\$</i> : Max aged LSA <i>\$ospfLsdbsid\$</i> type <i>\$ospfLsdBType\$</i> ifIndex <i>\$ospfLinkIfIdx\$</i> ifInstId <i>\$ospfLinkIfInstId\$</i> advertising router <i>\$ospfLsdBRtrId\$</i> |
| 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 1083: *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 1084: *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 <i>\$ospfRouterIdIpAddr\$</i> : Helper status for neighbor <i>\$ospfNbrIpAddr\$</i> router <i>\$ospfNbrRtrId\$</i> changed to <i>\$tmnxOspfNgNbrRestartHelperStatus\$</i> (Helper Age <i>\$tmnxOspfNgNbrRestartHelperAge\$</i> Exit Reason <i>\$tmnxOspfNgNbrRestartHelperExitRc\$</i>) |
| 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 1085: 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 <i>\$ospfRouterIdIpAddr\$</i> : Neighbor <i>\$ospfNbrRtrId\$</i> on <i>\$ospfNbrIpAddr\$</i> router state changed to <i>\$tmnxOspfNgNbrState\$</i> (event <i>\$ospfNbrEvent\$</i>) |
| 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 1086: *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 <i>\$tmnxOspfNgNbrRtrId\$</i> 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 1087: *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 <i>\$ospfRouterIdIpAddr\$</i> : NSSA translator state in area <i>\$ospfAreaId\$</i> changed to <i>\$tmnxOspfAreaNssaTranslatorState\$</i> |
| 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 1088: *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 <i>\$ospfRouterIdIpAddr\$</i> : Overload entered (event <i>\$tmnxOspfLastOverloadEnterCode\$</i>) <i>\$tmnxOspfNotifyDescription\$</i> |
| Cause | OSPF entered the overload state. <i>vRtrOspfLastOverloadEnterCode</i> holds the condition which caused OSPF to get into overload. |
| Effect | N/A |
| Recovery | N/A |

52.27 tmnxOspfOverloadExited

Table 1089: 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 \$tmnxOspfLastOverloadExitCode\$) |
| 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 1090: 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 <i>\$ospfRouterIdIpAddr\$</i> : Reached overload limit (event <i>\$tmnxOspfLastOverloadEnterCode\$</i>) <i>\$tmnxOspfNotifyDescription\$</i> |
| Cause | A <i>tmnxOspfOverloadWarning</i> trap is sent out when OSPF reaches 80 percent of overload limit. <i>tmnxOspfLastOverloadEnterCode</i> holds the condition which caused OSPF to approach this limit. |
| Effect | N/A |
| Recovery | N/A |

52.29 tmnxOspfRejectedAdjacencySet

Table 1091: *tmnxOspfRejectedAdjacencySet* properties

| Property name | Value |
|----------------------------------|---|
| Application name | OSPF |
| Event ID | 2059 |
| Event name | <i>tmnxOspfRejectedAdjacencySet</i> |
| SNMP notification prefix and OID | TIMETRA-OSPF-NG-MIB. <i>tmnxOspfNotifications.59</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Rejected adjacency set <i>\$tmnxOspfNotifyDescription\$</i> |
| Cause | The <i>tmnxOspfRejectedAdjacencySet</i> 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 1092: *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 1093: *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 <i>\$ospfRouterIdIpAddr\$</i> : Restart status changed to <i>\$tmnxOspfRestartStatus\$</i> (Restart Interval <i>\$tmnxOspfRestartInterval\$</i> Exit Reason <i>\$tmnxOspfRestartExitRc\$</i>) |
| 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 1094: *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 <i>\$tmnxOspfExportLimit\$</i> |
| Cause | Number of exported routes is dropped below the configured export limit. |
| Effect | N/A |
| Recovery | N/A |

52.33 tmnxOspfShamIfAuthFailure

Table 1095: *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 1096: *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 <i>\$ospfRouterIdIpAddr\$</i> : Conflicting configuration <i>\$tmnxOspfConfigErrorType\$</i> from sham-link neighbor <i>\$tmnxOspfShamIfRemoteNbrAddress\$</i> in <i>\$tmnxOspfPacketType\$</i> |
| 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 1097: 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 <i>\$ospfRouterIdIpAddr\$</i> : Bad packet, <i>\$tmnxOspfBadPacketErrType\$</i> , received from sham-link neighbor <i>\$tmnxOspfShamIfRemoteNbrAddress\$</i> in <i>\$tmnxOspfPacketType\$</i> |
| 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 1098: 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 1099: 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 <i>\$ospfRouterIdIpAddr\$</i> : Helper status for sham-link neighbor <i>\$tmnxOspfShamNbrRtrId\$</i> changed to <i>\$tmnxOspfShamNbrRestartHelperStatus\$</i> (Helper Age <i>\$tmnxOspfShamNbrRestartHelperAge\$</i> Exit Reason <i>\$tmnxOspfShamNbrRestartHelperExitRc\$</i>) |
| 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 1100: 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 <i>\$ospfRouterIdIpAddr\$</i> : State of sham-link neighbor <i>\$tmnxOspfShamNbrRtrId\$</i> changed to <i>\$tmnxOspfShamNbrState\$</i> |
| 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 1101: 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 | <p>Possible messages:</p> <ul style="list-style-type: none"> Statistics Index Allocation status changed to <i>\$tmnxOspfNotifStatsIndexStatus\$</i> for adjacency-set <i>\$tmnxOspfSidStatsAdjSet\$</i> Statistics Index Allocation status changed to <i>\$tmnxOspfNotifStatsIndexStatus\$</i> for adjacency interface <i>\$tmnxOspfSidStatsIfIndex\$</i> Statistics Index Allocation status changed to <i>\$tmnxOspfNotifStatsIndexStatus\$</i> for node <i>\$tmnxOspfSidStatsPrefix\$</i>/<i>\$tmnxOspfSidStatsPrefixLength\$</i> |
| 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 1102: 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 1103: 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 <i>\$ospfRouterIdIpAddr\$</i> : 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 1104: 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 <i>\$tmnxOspfRouterId\$</i> : Bad SRGB label range from router <i>\$tmnxOspfNotifSrgbAdvRtrID\$</i> in area <i>\$tmnxOspfNotifSrgbAreaId\$</i> : startLabel: <i>\$tmnxOspfNotifSrgbRangeStartLbl\$</i> maxIdx: <i>\$tmnxOspfNotifSrgbRangeMaxIdx\$</i> 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 1105: *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 <i>\$tmnxOspfSrPfxSid\$</i> , area <i>\$tmnxOspfSrPfxArea Id\$</i> , algo <i>\$tmnxOspfSrPfxSidAlgorithm\$</i> , reason: <i>\$tmnxOspfNotify Description\$</i> |
| 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 1106: *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 | <p>Possible messages:</p> <ul style="list-style-type: none"> SID not in range of router <i>\$tmnxOspfNotifPfxNhAdvRtr\$</i>: SID <i>\$tmnxOspfSrPfxSid\$</i>, area <i>\$tmnxOspfSrPfxAreaId\$</i>, algo <i>\$tmnxOspfSrPfxSidAlgorithm\$</i>, NO LABEL RANGE defined SID not in range of router <i>\$tmnxOspfNotifPfxNhAdvRtr\$</i>: SID <i>\$tmnxOspfSrPfxSid\$</i>, area <i>\$tmnxOspfSrPfxAreaId\$</i>, algo <i>\$tmnxOspfSrPfxSidAlgorithm\$</i>, startLbl <i>\$tmnxOspfNotifPfxSidRangeStartLbl\$</i>, maxIdx <i>\$tmnxOspfNotifPfxSidRangeMaxIdx\$</i> |
| 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 1107: 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 <i>\$ospfRouterIdIpAddr\$</i> : Packet failed <i>\$tmnxOspfConfigErrorType\$</i> authentication from virtual neighbor <i>\$ospfVirtIfNeighbor\$</i> area <i>\$ospfVirtIfAreaId\$</i> in <i>\$tmnxOspfPacketType\$</i> |
| 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 1108: 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 1109: 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 1110: 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 1111: 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 \$tmnxOspfVirtNbrRestartHelperExitReason\$) |
| 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 1112: 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 <i>\$ospfRouterIdIpAddr\$</i> : Virtual neighbor <i>\$ospfVirtNbrRtrId\$</i> in transit-area <i>\$ospfVirtNbrArea\$</i> state changed to <i>\$tmnxOspfVirtNbrState\$</i> (event <i>\$ospfVirtNbrEvent\$</i>) |
| 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 1113: 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 <i>\$tmnxPcapSessionName\$</i> 's allocated buffer is full, with size <i>\$tmnxPcapSessionBufferSize\$</i> . Total number of packets dropped by this session is <i>\$tmnxPcapSessionDroppedPackets\$</i> 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 1114: 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 <i>\$tmnxPcapSessionName\$</i> has encountered a buffer read/write failure. Total read failures: <i>\$tmnxPcapSessionBufReadFailures\$</i> , total write failures: <i>\$tmnxPcapSessionBufWriteFailures\$</i> . |
| 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 1115: 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 <i>\$tmnxPcapSessionName\$</i> has encountered a capture file operation related error. Session is in <i>\$tmnxPcapSessionState\$</i> 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 1116: 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 <i>\$tmnxPcapSessionName\$</i> has encountered a software failure. Session is in <i>\$tmnxPcapSessionState\$</i> 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 1117: 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 <i>\$tmnxPcepPccPeerAddr\$</i> state changed to <i>\$tmnxPcepPccPeerOperState\$</i> |
| 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 tmnxPfcplInvalidle

Table 1118: tmnxPfcplInvalidle properties

| Property name | Value |
|----------------------------------|--|
| Application name | PFCP |
| Event ID | 2001 |
| Event name | tmnxPfcplInvalidle |
| 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 <i>\$tmnxPfcplSeldHigh\$</i> : <i>\$tmnxPfcplSeldLow\$</i> : <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 tmnxPfcplNoSecondaryInterface

Table 1119: tmnxPfcplNoSecondaryInterface properties

| Property name | Value |
|------------------|-------|
| Application name | PFCP |
| Event ID | 2003 |

| Property name | Value |
|----------------------------------|--|
| Event name | tmnxPfcNoSecondaryInterface |
| 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 <i>\$tmnxPfcVRtrID</i> that is indicated in a PFCP request for session <i>\$tmnxPfcSeldHigh</i> <i>\$tmnxPfcSeldLow</i> does not exist: <i>\$tmnxSubAdditionalInfo</i> |
| 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 'tmnxPfcVRtrID', configure the secondary GTP interface with the object 'TIMETRA-WLAN-GW-MIB::tmnxGtpUpfDataEndptSecltfName'. |

55.3 tmnxPfcNoSuchCalltraceProfile

Table 1120: tmnxPfcNoSuchCalltraceProfile properties

| Property name | Value |
|----------------------------------|---|
| Application name | PFCP |
| Event ID | 2002 |
| Event name | tmnxPfcNoSuchCalltraceProfile |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.57 |
| Default severity | warning |
| Source stream | main |
| Message format string | Unknown calltrace trace-profile <i>\$tmnxSubNotifName</i> in PFCP request for session <i>\$tmnxPfcSeldHigh</i> <i>\$tmnxPfcSeldLow</i> : <i>\$tmnxSubAdditionalInfo</i> |
| 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 vRtrPimNgBierInbInvBfrld

Table 1121: vRtrPimNgBierInbInvBfrld properties

| Property name | Value |
|----------------------------------|---|
| Application name | PIM |
| Event ID | 2017 |
| Event name | vRtrPimNgBierInbInvBfrld |
| 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\$, \$vRtrPimNgNotifyBierInbGAddr\$) from IBBR \$vRtrPimNgNotifyBierInbIAddr\$ is dropped due to bfr-id mismatch, received bfr id \$vRtrPimNgNotifyBierInbInvBfrld\$. |
| 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 1122: 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 (<i>\$vRtrPimNgNotifyBierInbSAddr\$, \$vRtrPimNgNotifyBierInbGAddr\$</i>) from IBBR <i>\$vRtrPimNgNotifyBierInbIAddr\$</i> is dropped due to sub-domain mismatch, received sub domain id <i>\$vRtrPimNgNotifyBierInbInvSDId\$</i> . |
| 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 1123: 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 <i>\$vRtrPimNgAFGenBSRState\$</i> |
| 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 1124: 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 <i>\$vRtrPimNgDataMtIndex\$</i> configured for source address <i>\$vRtrPimNgDataMtMdSourceAddress\$</i> and group address <i>\$vRtrPimNgDataMtMdGroupAddress\$</i> has now <i>\$vRtrPimNgDataMtNumVpnSGs\$</i> or more C(S,G)s after being reused by C(S,G) (<i>\$DataMtCGrpSrcSourceAddr\$</i> , <i>\$DataMtCGrpSrcGroupAddr\$</i>) |
| 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 1125: 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 <i>\$vRtrPimNgNotifyMsgType\$</i> message on interface <i>\$vRtrIfIndex\$</i> for group <i>\$vRtrPimNgNotifyGroupAddr\$</i> 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 1126: 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 <i>\$vRtrPimNgIfNeighborAddress\$</i> on interface <i>\$vRtrIfIndex\$</i> 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 1127: 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 <i>\$vRtrIfIndex\$</i> as maximum of <i>\$vRtrPimNgIfNbrCount\$</i> 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 1128: 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 <i>\$vRtrPimNgIfNeighborAddress\$</i> on interface <i>\$vRtrIfIndex\$</i> |
| Cause | The PIM adjacency with a neighbor was lost. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

56.9 vRtrPimNgIfNeighborUp

Table 1129: 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 <i>\$vRtrPimNgIfNeighborAddress\$</i> on interface <i>\$vRtrIfIndex\$</i> came up |
| Cause | A PIM adjacency with a new neighbor was established. |
| Effect | N/A |
| Recovery | N/A |

56.10 vRtrPimNgInstMaxNbrReached

Table 1130: 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 <i>\$vRtrPimNgInstNbrCount\$</i> system pim neighbors reached. |
| Cause | The <i>vRtrPimNgInstMaxNbrReached</i> 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 1131: 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 <i>\$vRtrPimNgWrongMdtDefGrpAddr\$</i> from <i>\$vRtrPimNgNotifySourceIp\$</i> , expected <i>\$vRtrPimNgAFGenMdtDefGrpAddress\$</i> |
| Cause | The vRtrPimNgInvalidIPmsiTunnel event is generated when an invalid default core group address specified by vRtrPimNgWrongMdtDefGrpAddr 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 vRtrPimNgNotifySourceIp in the VPRN specified by vRtrPimNgWrongVprnId. The objects vRtrPimNgWrongPmsiP2mpld, vRtrPimNgWrongPmsiTunnelId and vRtrPimNgWrongPmsiExtTunlAddr in the event vRtrPimNgInvalidIPmsiTunnel are valid only when vRtrPimNgWrongPmsiType is 'rsvp (2)'. The objects vRtrPimNgWrongMdtDefGrpAddrType and vRtrPimNgWrongMdtDefGrpAddr in the event vRtrPimNgInvalidIPmsiTunnel are valid only when vRtrPimNgWrongPmsiType is either 'pimSsm (0)' or 'pimSm (1)'. The objects vRtrPimNgWrongPmsiLdpLspld, vRtrPimNgWrongPmsiSenderAdrTyp and vRtrPimNgWrongPmsiSenderAddr in the event vRtrPimNgInvalidIPmsiTunnel are valid only when vRtrPimNgWrongPmsiType is 'ldp (3)'. |

56.12 vRtrPimNgInvalidJoinPrune

Table 1132: 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 \$vRtrPimNgNotifySourceIp\$ with RP address \$vRtrPimNgNotifyWrongRPAddr\$ for group \$vRtrPimNgNotifyGroupAddr\$. Correct RP address for the group is \$vRtrPimNgNotifyRPAddr\$(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 1133: 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 <i>\$vRtrPimNgNotifySourceIp\$</i> with RP address <i>\$vRtrPimNgNotifyWrongRPAAddr\$</i> for group <i>\$vRtrPimNgNotifyGroupAddr\$</i> . Correct RP address for the group is <i>\$vRtrPimNgNotifyRPAAddr\$(0.0.0.0 if unknown)</i> |
| 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 1134: 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 <i>\$vRtrPimNgNumGraftRetriesExcd\$</i> retries for source address <i>\$vRtrPimNgNotifySourceAddr\$</i> , group address <i>\$vRtrPimNgNotifyGroupAddr\$</i> 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 1135: 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 <i>\$ifName\$</i> has exceeded the maximum limit of <i>\$vRtrPimNgIfMaxGroups\$</i> |
| 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 1136: 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 <i>\$vRtrPimNgNotifyGroupAddr\$</i> is dropped because of multicast CAC policy <i>\$vRtrPimNgIfMcacPolicyName\$</i> on interface <i>\$ifName\$</i> PIM instance <i>\$vRtrID\$</i> |
| 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 1137: 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 <i>\$vRtrID\$</i> , maximum selective provider tunnel limit of <i>\$vRtrPimNgGenMaxMmts\$</i> 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 1138: 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), (<i>\$vRtrPimNgNotifySourceIp\$</i> , <i>\$vRtrPimNgNotifyGroupAddr\$</i>) on IOM <i>\$tmnxCardHwIndex\$</i> , 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 1139: 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 <i>\$tmnx CardHwIndex\$</i> , 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 1140: 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 <i>\$vRtr PimNgUmhBMonTimeStamp\$</i> from the primary interface mpls-if- <i>\$v RtrPimNgUmhBMonPrimaryIfIndex\$</i> to the standby interface mpls-if- <i>\$vRtrPimNgUmhBMonStandbyIfIndex\$</i> when primary rate was <i>\$v</i> |

| Property name | Value |
|---------------|---|
| | <i>RtrPimNgUmhBMonPrimaryBW</i> and standby rate was <i>\$vRtrPimNgUmhBMonStandbyBW</i> . |
| Cause | The <i>vRtrPimNgUmhBMonFastFailPriToStb</i> 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 1141: 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 <i>\$vRtrPimNgUmhBMonTimeStamp</i> from the standby interface <i>mpls-if-\$vRtrPimNgUmhBMonStandbyIfIndex</i> to the primary interface <i>mpls-if-\$vRtrPimNgUmhBMonPrimaryIfIndex</i> when primary rate was <i>\$vRtrPimNgUmhBMonPrimaryBW</i> and standby rate was <i>\$vRtrPimNgUmhBMonStandbyBW</i> . |
| Cause | The <i>vRtrPimNgUmhBMonFastFailStbToPri</i> 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 1142: 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 <i>\$SvcId\$</i> with SAP <i>\$sapId\$</i> as maximum of <i>\$tmnxPimSnpgIntfNbrCount\$</i> 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 1143: 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 <i>\$tmnxPimSnpgIfNbrAddress\$</i> on <i>\$ifName\$</i> |
| Cause | The PIM adjacency with a neighbor was lost. |
| Effect | N/A |
| Recovery | N/A |

57.3 tmnxPimSnpgIfNeighborUp

Table 1144: *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 <i>\$tmnxPimSnpgIfNbrAddress\$</i> on <i>\$ifName\$</i> |
| Cause | The PIM adjacency with a new neighbor was established. |
| Effect | N/A |
| Recovery | N/A |

57.4 tmnxPimSnpgMaxNbrReached

Table 1145: *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 <i>\$SvcId\$</i> as maximum of <i>\$tmnxPimSnpgNbrCount\$</i> pim-snooping neighbor limit is reached. |
| Cause | The <i>tmnxPimSnpgMaxNbrReached</i> 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 1146: *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 <i>\$tmnxCardHwIndex\$</i> , 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 1147: *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 <i>\$tmnxPimSnpgGenOper State\$</i> . Configured mode is <i>\$tmnxPimSnpgGenMode\$</i> |
| 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 1148: 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: <ul style="list-style-type: none"> SFF DDM (<i>\$tmnxDDMFailedObject\$</i>) cleared SFF DDM Lane <i>\$tmnxDDMLaneIdOrModule\$</i> (<i>\$tmnxDDMFailedObject\$</i>) 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 1149: 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: <ul style="list-style-type: none"> SFF DDM (<i>\$tmnxDDMFailedObject\$</i>) raised SFF DDM Lane <i>\$tmnxDDMLaneIdOrModule\$</i> (<i>\$tmnxDDMFailedObject\$</i>) 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 1150: 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 <i>\$tmnxPortNotifyDS1AlarmReason\$</i> 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 1151: 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 <i>\$tmnxPortNotifyDS1AlarmReason\$</i> 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 1152: 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 ' <i>\$tmnxDS1Loopback\$</i> ' 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 1153: 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 1154: 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 <i>\$tmnxPortNotifyDS3AlarmReason\$</i> 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 1155: 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 <i>\$tmnxPortNotifyDS3AlarmReason\$</i> 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 1156: 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 1157: 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 1158: 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 (<i>\$tmnxDSXClockSyncStateObject\$</i>) |
| 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 1159: 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 <i>\$tmnxPortNotifyEtherAlarmReason\$</i> 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 1160: 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 <i>\$tmnxPortNotifyEtherAlarmReason\$</i> 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 1161: 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 <i>\$tmnxPortEtherDuplex\$</i> not compatible with MDA <i>\$tmnxMdaNotifyType\$</i> |
| 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 1162: 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 <i>\$tmnxMdaNotifyType\$</i> |
| 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 1163: 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 <i>\$tmnxPortNotifyPortId\$</i> |
| 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 1164: 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 <i>\$tmnxPortNotifyPortId\$</i> |
| 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 1165: 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 <i>\$tmnxPortEtherSpeed\$</i> not compatible with MDA <i>\$tmnxMdaNotifyType\$</i> |
| 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 1166: 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 <i>\$tmnxOtuIfAlarmState\$</i> |
| Cause | The <i>tmnxOtuIfAlarmNotification</i> 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 1167: 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 <i>\$tmnxPortNotifyError\$</i> |
| Cause | Generated when an error listed in tmnxPortNotifyError is detected on the port. |
| Effect | N/A |
| Recovery | N/A |

58.21 sdhLoopbackStart

Table 1168: 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 ' <i>\$tmnxSonetLoopback\$</i> ' 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 1169: *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 1170: *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 1171: 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 1172: 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 1173: 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 1174: 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 1175: 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 1176: 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 1177: 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 1178: 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 1179: 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 1180: 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 1181: 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 <i>\$tmnxPortNotifySonetAlarmReason\$</i> 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 1182: 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 <i>\$tmnxPortNotifySonetAlarmReason\$</i> 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 1183: 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 <i>\$tmnxPortNotifySonetPathAlarmReason\$</i> 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 1184: 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 <i>\$tmnxPortNotifySonetPathAlarmReason\$</i> 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 1185: 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 <i>\$tmnxPortPortID\$</i> Authorized - CBSID Id: <i>\$tmnxCellPortCbsdAuthId\$</i> , Grant Id: <i>\$tmnxCellPortCbsdAuthGrantId\$</i> , Grant expire time: <i>\$tmnxCellPortCbsdAuthGrantExpTime\$</i> , Heartbeat interval: <i>\$tmnxCellPortCbsdAuthHeartbeatInt\$</i> seconds |
| Cause | The tmnxCellPortCbsdAuthorized notification is generated when the CBSID is authorized by the SAS. |
| Effect | The CBSID enables SR-OS on the cellular interface. |
| Recovery | Not applicable. |

58.39 tmnxCellPortCbsdGranted

Table 1186: tmnxCellPortCbsdGranted properties

| Property name | Value |
|----------------------------------|--|
| Application name | PORT |
| Event ID | 2079 |
| Event name | tmnxCellPortCbsdGranted |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeellularNotifications.8 |
| Default severity | minor |
| Source stream | main |
| Message format string | CBSD <i>\$tmnxPortPortID\$</i> Granted - CBSID Id: <i>\$tmnxCellPortCbsdAuthId\$</i> , Grant Id: <i>\$tmnxCellPortCbsdAuthGrantId\$</i> , Grant expire time: <i>\$tmnxCellPortCbsdAuthGrantExpTime\$</i> , Heartbeat interval: <i>\$tmnxCellPortCbsdAuthHeartbeatInt\$</i> seconds |
| Cause | The tmnxCellPortCbsdGranted notification is generated when the CBSID has received a grant Id from the SAS. The CBSID is not authorized until after the authorized notification is generated. |
| Effect | The CBSID is awaiting authorization from the SAS. |
| Recovery | Not applicable. |

58.40 tmnxCellPortCbsdRegistered

Table 1187: tmnxCellPortCbsdRegistered properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2077 |
| Event name | tmnxCellPortCbsdRegistered |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeIularNotifications.6 |
| Default severity | minor |
| Source stream | main |
| Message format string | CBSD <i>\$tmnxPortPortID\$</i> Registered - CBSD Id: <i>\$tmnxCellPortCbsdAuthId\$</i> , Server: <i>\$tmnxCellPortCbsdAuthCurSasSvrlp\$</i> |
| 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 1188: tmnxCellPortCbsdTransDown properties

| Property name | Value |
|----------------------------------|--|
| Application name | PORT |
| Event ID | 2081 |
| Event name | tmnxCellPortCbsdTransDown |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeIularNotifications.10 |
| Default severity | minor |
| Source stream | main |

| Property name | Value |
|-----------------------|--|
| Message format string | CBSD <i>\$tmnxPortPortID\$</i> transitioned from <i>\$tmnxCellCbsdAuthPrevTransState\$</i> to <i>\$tmnxCellCbsdAuthNewTransState\$</i> - CBSID Id: <i>\$tmnxCellPortCbsdAuthId\$</i> , Grant Id: <i>\$tmnxCellPortCbsdAuthGrantId\$</i> , Reason: <i>\$tmnxCellCbsdAuthFailReason\$</i> , Response code: <i>\$tmnxCellCbsdAuthRespCode\$</i> |
| Cause | The tmnxCellPortCbsdTransDown notification is generated when the CBSID is transitioning to a lower state. |
| Effect | The CBSID proceeds to complete authorization with the SAS from the state the CBSID has transitioned to. |
| Recovery | Not applicable. |

58.42 tmnxCellPortCbsdUnregistered

Table 1189: 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 <i>\$tmnxPortPortID\$</i> Unregistered - CBSID Id: <i>\$tmnxCellPortCbsdAuthId\$</i> , Reason: <i>\$tmnxCellCbsdAuthFailReason\$</i> , Response code: <i>\$tmnxCellCbsdAuthRespCode\$</i> |
| Cause | The tmnxCellPortCbsdUnregistered notification is generated when the CBSID is declared unregistered with the SAS. |
| Effect | The CBSID restarts the registration procedures with the SAS. |
| Recovery | Not applicable. |

58.43 tmnxCellularActiveSimChange

Table 1190: tmnxCellularActiveSimChange properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2070 |
| Event name | tmnxCellularActiveSimChange |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeIlIarNotificatiOns.5 |
| Default severity | major |
| Source stream | main |
| Message format string | Active SIM card switched to SIM <i>\$tmnxCellMdaOperActiveSim\$</i> (<i>\$tmnxCellMdaSimLastSwitchReason\$</i>) |
| 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 1191: tmnxCellularBearerCreated properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2065 |
| Event name | tmnxCellularBearerCreated |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeIlIarNotificatiOns.1 |
| Default severity | warning |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | Dedicated bearer id <i>\$tmnxCellPortBearerId\$</i> created on port <i>\$tmnxPortPortID\$</i> |
| 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 1192: tmnxCellularBearerDeleted properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2066 |
| Event name | tmnxCellularBearerDeleted |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeellularNotifications.2 |
| Default severity | warning |
| Source stream | main |
| Message format string | Dedicated bearer id <i>\$tmnxCellPortBearerId\$</i> deleted on port <i>\$tmnxPortPortID\$</i> |
| 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 1193: *tmnxCellularBearerModified* properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2067 |
| Event name | tmnxCellularBearerModified |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeellularNotifications.3 |
| Default severity | warning |
| Source stream | main |
| Message format string | Bearer id <i>\$tmnxCellPortBearerId\$</i> modified on port <i>\$tmnxPortPortID\$</i> |
| 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 1194: *tmnxCellularNoServiceReset* properties

| Property name | Value |
|----------------------------------|--|
| Application name | PORT |
| Event ID | 2069 |
| Event name | tmnxCellularNoServiceReset |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeellularNotifications.4 |
| Default severity | critical |
| Source stream | main |
| Message format string | Could not establish service over the cellular port (<i>\$tmnxCellMdaNoServiceResetReason\$</i>). 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 1195: tmnxCellularRssiAlarm properties

| Property name | Value |
|----------------------------------|--|
| Application name | PORT |
| Event ID | 2085 |
| Event name | tmnxCellularRssiAlarm |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeIlularNotifications.11 |
| Default severity | minor |
| Source stream | main |
| Message format string | The RSSI level detected by cellular port <i>\$tmnxPortNotifyPortId\$</i> has been below the threshold <i>\$tmnxCellSimCardRssiThresh\$</i> dBm for the duration of <i>\$tmnxCellSimCardRssiAlarmTime\$</i> 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 1196: *tmnxCellularRssiAlarmClear* properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2086 |
| Event name | tmnxCellularRssiAlarmClear |
| SNMP notification prefix and OID | TIMETRA-CELLULAR-MIB.tmnxCeellularNotifications.12 |
| Default severity | cleared |
| Source stream | main |
| Message format string | Alarm tmnxCellularRssiAlarm is cleared - The RSSI level detected by cellular port <i>\$tmnxPortNotifyPortId\$</i> has been equal to or above the threshold <i>\$tmnxCellSimCardRssiThresh\$</i> dBm for the duration of <i>\$tmnxCellSimCardRssiAlarmTime\$</i> seconds |
| Cause | After the tmnxCellularRssiAlarm is generated, the tmnxCellularRssiAlarmClear 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 1197: *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 1198: 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 1199: 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: <i>\$tmnxCohOptPortAlarmState\$</i> |
| 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 tmnxCohOptPortDefectPoints. 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 1200: 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 <i>\$tmnxPortNotifyEtherCrcAlarm Value\$</i> threshold <i>\$tmnxPortNotifyEtherCrcMultiplier\$*10e-\$tmnxPort NotifyEtherCrcThreshold\$</i> 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 1201: 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 <i>\$tmnxPortNotifyEtherCrcAlarm Value\$</i> threshold <i>\$tmnxPortNotifyEtherCrcMultiplier\$*10e-\$tmnxPort NotifyEtherCrcThreshold\$</i> 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 1202: 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 <i>\$tmnxNotifyPortId\$</i> oper egress rate has changed to <i>\$tmnxPortEtherOperEgressRate\$</i> 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 1203: 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 1204: 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 1205: 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 <i>\$tmnxPortNotifyEtherSym AlarmValue\$</i> threshold <i>\$tmnxPortNotifyEtherSymMultiplier\$*10e-\$tmnxPortNotifyEtherSymThreshold\$</i> 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 1206: 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 <i>\$tmnxPortNotifyEtherSym AlarmValue\$</i> threshold <i>\$tmnxPortNotifyEtherSymMultiplier\$*10e-\$tmnxPortNotifyEtherSymThreshold\$</i> 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 1207: 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 <i>\$tmnxPortFlexEGrpAlmReason\$</i> 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 1208: 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 <i>\$tmnxPortFlexEGrpAlmReason\$</i> 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 1209: 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 <i>\$tmnxPortFlexEMbrPhyInstAlmReason\$</i> 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 1210: 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 <i>\$tmnxPortFlexEMbrPhyInstAlmReason\$</i> 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 1211: *tmnxEqPortFlexEMemberAlm* properties

| Property name | Value |
|----------------------------------|--|
| Application name | PORT |
| Event ID | 2099 |
| Event name | tmnxEqPortFlexEMemberAlm |
| SNMP notification prefix and OID | TIMETRA-PORT-MIB.tmnxPortNotification.80 |
| Default severity | minor |
| Source stream | main |
| Message format string | Alarm <i>\$tmnxPortFlexEMbrAlmReason\$</i> 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 tmnxEqPortFlexEMemberAlmClr

Table 1212: *tmnxEqPortFlexEMemberAlmClr* properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2100 |
| Event name | tmnxEqPortFlexEMemberAlmClr |
| SNMP notification prefix and OID | TIMETRA-PORT-MIB.tmnxPortNotification.81 |
| Default severity | minor |
| Source stream | main |
| Message format string | Alarm <i>\$tmnxPortFlexEMbrAlmReason\$</i> 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 1213: *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 <i>\$tmnxSonetClockSource\$</i> not compatible with MDA type <i>\$tmnxMdaNotifyType\$</i> |
| 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 1214: *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 <i>\$tmnxSonetFraming\$</i> not compatible with MDA type <i>\$tmnxMdaNotifyType\$</i> |
| Cause | Notification <i>tmnxEqSonetFramingNotCompatible</i> 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 1215: *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 <code>tmnxEqSonetSfThreshNotCompatible</code> 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 1216: *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 <code>tmnxHwAggShpSchedOperColorAmber</code> 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 1217: 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 1218: 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 1219: 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 <i>\$tmnxPort NotifyAUIResetSource\$</i> |
| 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 1220: 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 \$tmnxPortPortID\$ |
| 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 1221: 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 \$tmnxPortPortID\$ |
| Cause | The tmnxPortEtherLoopbackStopped notification is generated when a loopback is removed on an Ethernet port. The value of tmnxPortEtherLoopback 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 1222: 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 \$tmnxPortGnssSyncStatus\$, 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 1223: 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 <i>\$tmnxPortNotifyPortId\$</i> that it cannot support - <i>\$tmnxPortNotifyDescription\$</i> |
| 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 1224: 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= <i>\$tmnxObjType\$</i> Owner= <i>\$tmnxObjPortId\$</i> Type= <i>\$tmnxObjAppType\$</i> Pool= <i>\$tmnxObjAppPool\$</i> ResvSize= <i>\$tmnxObjAppResvSize\$</i> SumOfQ ResvSize= <i>\$tmnxObjAppSumOfQResvSize\$</i> Old ResvCBS= <i>\$tmnxObjAppResvCbsOld\$</i> New ResvCBS= <i>\$tmnxObjAppResvCbsNew\$</i> Old ResvSize= <i>\$tmnxObjAppResvSizeOld\$</i> |
| 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 1225: 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= <i>\$tmnxObjType\$</i> Owner= <i>\$tmnxObjPortId\$</i> Type= <i>\$tmnxObjAppType\$</i> Pool= <i>\$tmnxObjAppPool\$</i> ResvSize= <i>\$tmnxObjAppResvSize\$</i> SumOfQ ResvSize= <i>\$tmnxObjAppSumOfQResvSize\$</i> Old ResvCBS= <i>\$tmnxObjAppResvCbsOld\$</i> New ResvCBS= <i>\$tmnxObjAppResvCbsNew\$</i> Old ResvSize= <i>\$tmnxObjAppResvSizeOld\$</i> |
| 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 1226: 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 1227: 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 <code>tmnxResvPoolUseThreshExcd</code> 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 1228: `tmnxResvPoolUseThreshNotExcd` properties

| Property name | Value |
|----------------------------------|---|
| Application name | PORT |
| Event ID | 2092 |
| Event name | <code>tmnxResvPoolUseThreshNotExcd</code> |
| 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 <code>tmnxResvPoolUseThreshNotExcd</code> 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 1229: 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 <i>\$tmnxPortNotifyPortId\$</i> control leads signal change: <i>\$tmnxPortNotifyLeadsSignalChg\$</i> |
| 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 1230: 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 <i>\$tmnxPortNotifyPortId\$</i> squelch reset issued, existing squelch status: <i>\$tmnxRS232SocketSquelchStatus\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

58.84 tmnxRS232SquelchStatusChange

Table 1231: *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 <i>\$tmnxPortNotifyPortId\$</i> squelch status: <i>\$tmnxRS232SocketSquelchStatus\$</i> |
| 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, <i>tmnxRS232SocketSquelchDelay</i> . 2) The continuous stream of data is no longer being received for a specified period of time, <i>tmnxRS232SocketUnsquelchDelay</i> . |
| 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 1232: *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 1233: *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 1234: 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 1235: *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 1236: *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 <i>\$tmnxWlanNotifyWlanNetworkId\$</i> SSID ' <i>\$tmnxWlanNetworkSSID\$</i> ' |
| Cause | The system generates a <i>tmnxWlanNetworkConnected</i> notification when the system establishes a WLAN connection to the specified network. |
| Effect | N/A |
| Recovery | N/A |

58.90 *tmnxWlanNetworkDisconnected*

Table 1237: *tmnxWlanNetworkDisconnected* properties

| Property name | Value |
|----------------------------------|--|
| Application name | PORT |
| Event ID | 2075 |
| Event name | <i>tmnxWlanNetworkDisconnected</i> |
| SNMP notification prefix and OID | TIMETRA-WLAN-MIB. <i>tmnxWlanNotifications.2</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Disconnected from WLAN network <i>\$tmnxWlanNotifyWlanNetworkId\$</i> SSID ' <i>\$tmnxWlanNetworkSSID\$</i> ' |
| Cause | The system generates a <i>tmnxWlanNetworkDisconnected</i> notification when the system loses the WLAN connection to the specified network. |
| Effect | N/A |
| Recovery | N/A |

58.91 *tPortAccEgrQGrpHostMatchFailure*

Table 1238: 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 1239: 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 |
|---------------|--|
| | <i>OrgString\$</i> and sub-id ' <i>\$tmnxHostMatchNotifySubIdent\$</i> ' on port <i>\$tmnxPortNotifyPortId\$</i> |
| 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 1240: 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 <i>\$tmnxMlpppBundle Indictors\$ - \$tmnxPppoeNotifyDescription\$</i> . |
| 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 lfiCfg' to 'lfiCfg', Link Fragmentation and Interleaving (LFI) is disabled on the bundle. |
| Recovery | N/A |

59.2 tmnxPppoeLacFragFailed

Table 1241: tmnxPppoeLacFragFailed properties

| Property name | Value |
|------------------|-------|
| Application name | PPPOE |

| Property name | Value |
|----------------------------------|---|
| Event ID | 2008 |
| Event name | tmnxPppoeLacFragFailed |
| SNMP notification prefix and OID | TIMETRA-PPPOE-MIB.tmnxPppoeNotifications.8 |
| Default severity | warning |
| Source stream | main |
| Message format string | LAC fragmentation failed on session <i>\$tmnxPppoeLacSteeringSession\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> within L2TP router <i>\$tmnxPppoeLacFragVRtrID\$</i> using FPE id <i>\$tmnxPppoeLacFragFpeld\$</i> (<i>\$tmnxPppoeLacSteeringFailure\$</i>). |
| Cause | The tmnxPppoeLacFragFailed notification indicates the FPE resources, required for LAC fragmentation, are not available or the FPE path is not operational. The object tmnxPppoeLacSteeringFailure describes the problem. |
| Effect | N/A |
| Recovery | N/A |

59.3 tmnxPppoeLacSteeringActive

Table 1242: tmnxPppoeLacSteeringActive properties

| Property name | Value |
|----------------------------------|--|
| Application name | PPPOE |
| 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 <i>\$tmnxPppoeLacSteeringSession\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclD\$</i> is steered using profile <i>\$tmnxPppoeLacSteeringProfile\$</i> . |
| Cause | The tmnxPppoeLacSteeringActive notification indicates that the appropriate PPPoE/LAC session is steered. |

| Property name | Value |
|---------------|-------|
| Effect | N/A |
| Recovery | N/A |

59.4 tmnxPppoeLacSteeringFailed

Table 1243: 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 <i>\$tmnxPppoeLacSteeringSession\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svcl\$</i> changed to steering failed using profile <i>\$tmnxPppoeLacSteeringProfile\$</i> (<i>\$tmnxPppoeLacSteeringFailure\$</i>). |
| Cause | The tmnxPppoeLacSteeringFailed notification indicates that steering has failed. The problem is described in the object tmnxPppoeLacSteeringFailure. |
| Effect | N/A |
| Recovery | N/A |

59.5 tmnxPppoeLacSteeringStopped

Table 1244: tmnxPppoeLacSteeringStopped properties

| Property name | Value |
|------------------|-------|
| Application name | PPPOE |

| Property name | Value |
|----------------------------------|---|
| 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 <i>\$tmnxPppoeLacSteeringSession\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> has stopped steering using profile <i>\$tmnxPppoeLacSteeringProfile\$</i> . |
| 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 |

59.6 tmnxPppoeMaxSessionsOvrExceeded

Table 1245: *tmnxPppoeMaxSessionsOvrExceeded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | PPPOE |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxPppoeMaxSessionsOvrReason\$</i> |
| Cause | The tmnxPppoeMaxSessionsOvrExceeded notification indicates the configured maximum number of sessions has been reached. Detailed information is provided in the object tmnxPppoeMaxSessionsOvrReason. |

| Property name | Value |
|---------------|---------------------------|
| Effect | N/A |
| Recovery | No recovery is necessary. |

59.7 tmnxPppoeNcpFailure

Table 1246: *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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxPppoeNcpFailureReason\$</i> |
| Cause | The system could not handle a NCP phase for a PPPoE session. The problem is described in the managed object tmnxPppoeNcpFailure Reason. |
| Effect | N/A |
| Recovery | N/A |

59.8 tmnxPppoeSessionFailure

Table 1247: *tmnxPppoeSessionFailure* properties

| Property name | Value |
|------------------|-------|
| Application name | PPPOE |
| Event ID | 2001 |

| Property name | Value |
|----------------------------------|---|
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxPppoeSessionFailureReason\$</i> |
| Cause | The system could not create a new PPPoE session in the tmnxPppoeSessionTable. The problem is described in the managed object tmnxPppoeSessionFailureReason. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

60 PPPOE_CLNT

60.1 tmnxPppoeClientEchoTimeout

Table 1248: 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 <i>\$tmnxPppoeClntIdent\$</i> 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 1249: 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 <i>\$tmnxPppoeClntIdent\$</i> - protocol <i>\$tmnxPppoeNcpFailureProtocol\$</i> |
| 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 1250: 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 <i>\$tmnxPppoeClntIdent\$</i> |
| 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 1251: 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 <i>\$tmnxCpmCardSlotNum\$</i> 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 1252: *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 <i>\$tmnxCpmCardSlotNum\$</i> 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 1253: *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: <i>\$tmnxPtpClockRecovery State\$</i> |

| 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 1254: 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) <i>\$tmnxPtpNotifyRowDescription\$</i> |
| 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 1255: 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 <i>\$tmnxPtpMasterClockAddress\$</i> , Old Parent <i>\$tmnxPtpMasterClockLastIpAddress\$</i> . |
| 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 1256: 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 <i>\$tmnxChassisNotifyHwIndex\$</i> 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. <code>tmnxPtpOutOfResourcesClear</code> is generated when this event is cleared. |
| Effect | N/A |
| Recovery | N/A |

61.7 `tmnxPtpOutOfResourcesClear`

Table 1257: `tmnxPtpOutOfResourcesClear` properties

| Property name | Value |
|----------------------------------|---|
| Application name | PTP |
| Event ID | 2006 |
| Event name | <code>tmnxPtpOutOfResourcesClear</code> |
| SNMP notification prefix and OID | TIMETRA-PTP-MIB. <code>tmnxPtp1588Notifications.6</code> |
| Default severity | minor |
| Source stream | main |
| Message format string | IEEE1588 (PTP) Card <code>\$tmnxChassisNotifyHwIndex\$</code> out of resources cleared |
| Cause | The <code>tmnxPtpOutOfResourcesClear</code> 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 1258: *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 <i>\$tmnxPtpPeer IpAddress\$</i> is performed at the CPM. Performance may be degraded. |
| Cause | The <i>tmnxPtpPeerNoRxTimestamping</i> 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)'. The <i>tmnxPtpPeerNoRxTimestamping</i> 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 than 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 1259: *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 <i>\$tmnxPtpPeer IpAddress\$</i> is now performed at the port. |
| Cause | The <i>tmnxPtpPeerNoRxTimestampingClear</i> notification is generated when the conditions that caused the <i>tmnxPtpPeerNoRxTimestamping</i> 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 1260: *tmnxPtpPeerNoTxTimestamping* properties

| Property name | Value |
|----------------------------------|--|
| Application name | PTP |
| Event ID | 2013 |
| Event name | <i>tmnxPtpPeerNoTxTimestamping</i> |
| SNMP notification prefix and OID | TIMETRA-PTP-MIB. <i>tmnxPtp1588Notifications.13</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Timestamping of transmit communications with peer <i>\$tmnxPtpPeer IpAddress\$</i> is performed at the CPM. Performance may be degraded. |
| Cause | The <i>tmnxPtpPeerNoTxTimestamping</i> 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 than 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 1261: *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 <i>\$tmnxPtpPeerIpAddress\$</i> 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)'. 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 1262: *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 <i>\$tmnxPtpNotifyPortId\$</i> 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 1263: *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 <i>\$tmnxPortPortID\$</i> neighbor <i>\$tmnxPtpPortNeighborMacAddress\$</i> 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 1264: 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 <i>\$tmnxPtpClockClockType\$</i> , profile <i>\$tmnxPtpClockProfile\$</i>) is different than the initial configuration (clock-type <i>\$tmnxPtpNotifyInitialClockType\$</i> , profile <i>\$tmnxPtpNotifyInitialProfile\$</i>). 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 1265: *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 <i>tmnxPtpRequiresSystemRebootClear</i> 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 1266: *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: <i>\$tmnxPtpTimeRecoveryState\$</i> |

| 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 1267: *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 ' <i>\$tmnxPythonNotifyInterpreter\$</i> ' has restarted - <i>\$tmnxPythonNotifyString\$</i> |
| 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 1268: 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 <i>\$tmnxRadSrvPlcyName\$</i> after <i>\$tmnxRadSrvPlcyAcctOnOffRetryCnt\$</i> retries <i>\$tmnxRadiusAdditionalInfo\$</i> |
| 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 1269: 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 : <i>\$tmnxRadiusAdditionalInfo\$</i> |
| 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 1270: 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= <i>\$tmnxRadius NotifyAddr\$</i>) in RADIUS server policy name changed to <i>\$tmnxRadSrv PlcySrvOperState\$</i> |
| 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 tmnxRadSrvPlcyAlgorithm. - after the time specified in the object tmnxRadSrvPlcyDownTime 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 1271: 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 <i>\$ripPacketSrcIp\$</i> received on interface <i>\$vRtrIfIndex\$</i> because <i>\$ripPacketDiscardReason\$</i> |
| 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 1272: 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 <i>\$vRtrRipPeerAddress\$</i> on interface <i>\$vRtrRipPeerIfIndex\$</i> |
| 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 1273: 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 <i>\$vRtrRipPeerAddress\$</i> on interface <i>\$vRtrRipPeerIfIndex\$</i> |
| 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 1274: 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 1275: 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 <code>\$vRtrRipInstanceExpLmtLogPercent\$</code> percent of the export limit <code>\$vRtrRipInstanceExportLimit\$</code> |
| 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 1276: 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 1277: *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 <i>\$vRtrRipInstanceExportLimit\$</i> |
| Cause | Number of exported routes is dropped below the configured export limit. |
| Effect | N/A |
| Recovery | N/A |

64.8 vRtrRipInstanceShuttingDown

Table 1278: *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 <i>\$ripInstanceShuttingDownReason\$</i> |
| 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 1279: 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 <i>\$vRtrRipPeerAddress\$</i> on interface <i>\$vRtrRipPeerIfIndex\$</i> 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 1280: 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 <i>\$tmnxRipNgInstVersion\$</i> packet received from peer <i>\$tmnxRipNgPeerAddress\$</i> on interface <i>\$tmnxRipNgPeerIfIndex\$</i> |
| 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 1281: 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 <i>\$tmnxRipNgInstVersion\$</i> packet received from peer <i>\$tmnxRipNgPeerAddress\$</i> on interface <i>\$tmnxRipNgPeerIfIndex\$</i> |
| 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 1282: 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 | <i>\$tmnxRipNgInstVersion\$</i> neighbor <i>\$vRtrIfIndex\$</i> 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 1283: 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 | <i>\$tmnxRipNgInstVersion\$</i> instance has reached the export limit <i>\$tmnxRipNgInstExportLimit\$</i> , 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 1284: 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 | <i>\$tmnxRipNgInstVersion\$</i> instance has reached <i>\$tmnxRipNgInstExpLmtLogPct\$</i> percent of the export limit <i>\$tmnxRipNgInstExportLimit\$</i> |
| Cause | A <i>tmnxRipNgInstExpLmtWarning</i> notification is generated when the number of exported routes is equal to the configured percent, <i>tmnxRipNgInstExpLmtLogPct</i> of the export limit, <i>tmnxRipNgInstExportLimit</i> . 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 1285: *tmnxRipNgInstRestarted* properties

| Property name | Value |
|----------------------------------|--|
| Application name | RIP_NG |
| Event ID | 2005 |
| Event name | <i>tmnxRipNgInstRestarted</i> |
| SNMP notification prefix and OID | TIMETRA-RIP-NG-MIB. <i>tmnxRipNgNotifications.4</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | <i>\$tmnxRipNgInstVersion\$</i> 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 <i>tmnxRipNgInstRestarted</i> trap is generated when the RIP instance has restarted. |
| Effect | N/A |
| Recovery | N/A |

65.7 tmnxRipNgInstRtsExpLmtDropped

Table 1286: *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 <i>\$tmnxRipNgInstVersion\$</i> instance has dropped below the export limit <i>\$tmnxRipNgInstExportLimit\$</i> |
| 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 1287: *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 | <i>\$tmnxRipNgInstVersion\$</i> instance is being operationally 'shutdown' because <i>\$tmnxRipNgNotifyReason\$</i> |
| Cause | A <i>tmnxRipNgInstShuttingDown</i> 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 1288: *tmnxRipNgPacketDiscarded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | RIP_NG |
| Event ID | 2001 |
| Event name | <i>tmnxRipNgPacketDiscarded</i> |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | main |
| Message format string | Discarded <i>\$tmnxRipNgInstVersion\$</i> packet received from <i>\$tmnxRipNgNotifySrcAddr\$</i> on interface <i>\$vRtrIfIndex\$</i> because <i>\$tmnxRipNgNotifyReason\$</i> |
| 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 1289: 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 | <i>\$tmnxRipNgInstVersion\$ peer \$tmnxRipNgPeerAddress\$ on interface \$tmnxRipNgPeerIfIndex\$ went down due to a BFD session failure</i> |
| 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 1290: 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 1291: 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 <i>\$tmnxRpkiPeerAddr\$</i> changed to <i>\$tmnxRpkiTrap Status\$</i> due to <i>\$tmnxRpkiErrorType\$</i> |
| 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 1292: *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 : <i>\$tmnxRpkiPeerAddr\$</i> |
| 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 vRtrRsvplfNbrStateDown

Table 1293: vRtrRsvplfNbrStateDown properties

| Property name | Value |
|----------------------------------|---|
| Application name | RSVP |
| Event ID | 2004 |
| Event name | vRtrRsvplfNbrStateDown |
| SNMP notification prefix and OID | TIMETRA-RSVP-MIB.tmnxRsvpNotifications.4 |
| Default severity | warning |
| Source stream | main |
| Message format string | Neighbor <i>\$vRtrRsvpNbrAddress\$</i> on interface <i>\$ifIndex\$</i> changed to inactive state because <i>\$vRtrRsvplfNbrDownReasonCode\$</i> |
| Cause | A RSVP interface neighbor changed to the inactive state. |
| Effect | N/A |
| Recovery | N/A |

68.2 vRtrRsvplfNbrStateUp

Table 1294: vRtrRsvplfNbrStateUp properties

| Property name | Value |
|----------------------------------|--|
| Application name | RSVP |
| Event ID | 2003 |
| Event name | vRtrRsvplfNbrStateUp |
| SNMP notification prefix and OID | TIMETRA-RSVP-MIB.tmnxRsvpNotifications.3 |

| Property name | Value |
|-----------------------|--|
| Default severity | warning |
| Source stream | main |
| Message format string | Neighbor <i>\$vRtrRsvpNbrAddress\$</i> on interface <i>\$ifIndex\$</i> changed to active state |
| Cause | A RSVP interface neighbor changed to the active state. |
| Effect | N/A |
| Recovery | N/A |

68.3 vRtrRsvplfStateChange

Table 1295: vRtrRsvplfStateChange properties

| Property name | Value |
|----------------------------------|---|
| Application name | RSVP |
| Event ID | 2002 |
| Event name | vRtrRsvplfStateChange |
| SNMP notification prefix and OID | TIMETRA-RSVP-MIB.tmnxRsvpNotifications.2 |
| Default severity | warning |
| Source stream | main |
| Message format string | Interface <i>\$ifIndex\$</i> is in administrative state <i>\$rsvplfEnabled\$</i> , operational state <i>\$vRtrRsvplfOperState\$</i> |
| Cause | A RSVP interface changed state. |
| Effect | Service is affected. |
| Recovery | No recovery is required. |

68.4 vRtrRsvpPEFailOverPriToStdBy

Table 1296: 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 \$vRtrPimNgMvpnUMHPEStandbyAddr\$ due to \$vRtrRsvpPEFailOverReasonCode\$ |
| 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 vRtrPimNgMvpnUMHPEAddrType and vRtrPimNgMvpnUMHPEAddr indexes of the varbinds in this notification. |
| Effect | The tunnel traffic may be affected. |
| Recovery | None required. |

68.5 vRtrRsvpPEFailOverStdByToPri

Table 1297: 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 <i>\$vRtrID\$</i> from standby PE <i>\$vRtrPimNgMvpnUMHPEStandbyAddr\$</i> to primary PE <i>\$vRtrPimNgMvpnUMHPEAddr\$</i> |
| 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 1298: 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 <i>\$vRtrRsvpGeneralAdminState\$</i> , operational state <i>\$vRtrRsvpGeneralOperState\$</i> |
| Cause | The RSVP module changed state. |
| Effect | Service is affected. |
| Recovery | No recovery is required. |

69 SATELLITE

69.1 tmnxSatelliteOperStateChange

Table 1299: 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: <ul style="list-style-type: none"> • <i>\$tmnxHwIndex\$</i> is in <i>\$tmnxHwOperState\$</i> state - <i>\$tmnxSatNotifyFailureReason\$</i> • <i>\$tmnxHwIndex\$</i> is in <i>\$tmnxHwOperState\$</i> 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 1300: *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 <i>\$tmnxSatLocalForwardId\$</i> SAP <i>\$tmnxSatPortId\$</i> : <i>\$tmnxSatEncapValue\$</i> changed to administrative state: <i>\$tmnxSatLocalForwardSapAdminState\$</i> , operational state: <i>\$tmnxSatLocalForwardSapOperState\$</i> |
| 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 1301: *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 <i>\$tmnxSatLocalForwardId\$</i> changed to administrative state: <i>\$tmnxSatLocalForwardAdminState\$</i> , operational state: <i>\$tmnxSatLocalForwardOperState\$</i> |
| 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 tmnxSatSynclfTimHoldover

Table 1302: tmnxSatSynclfTimHoldover properties

| Property name | Value |
|----------------------------------|--|
| Application name | SATELLITE |
| Event ID | 2006 |
| Event name | tmnxSatSynclfTimHoldover |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.6 |
| Default severity | critical |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxHwIndex\$</i> is in holdover state |
| Cause | The tmnxSatSynclfTimHoldover 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 tmnxSatSynclfTimHoldoverClear

Table 1303: tmnxSatSynclfTimHoldoverClear properties

| Property name | Value |
|----------------------------------|---|
| Application name | SATELLITE |
| Event ID | 2007 |
| Event name | tmnxSatSynclfTimHoldoverClear |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.7 |
| Default severity | cleared |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxHwIndex\$</i> , holdover state cleared |
| Cause | The tmnxSatSynclfTimHoldoverClear 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 tmnxSatSynclfTimRef1Alarm

Table 1304: tmnxSatSynclfTimRef1Alarm properties

| Property name | Value |
|------------------|-----------|
| Application name | SATELLITE |
| Event ID | 2008 |

| Property name | Value |
|----------------------------------|---|
| Event name | tmnxSatSynclfTimRef1Alarm |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.8 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxHwIndex\$</i> , alarm <i>\$tmnxSatNotifySynclfTimRefAlarm\$</i> on reference 1 |
| Cause | The tmnxSatSynclfTimRef1Alarm 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 tmnxSatSynclfTimRef1AlarmClear

Table 1305: tmnxSatSynclfTimRef1AlarmClear properties

| Property name | Value |
|----------------------------------|---|
| Application name | SATELLITE |
| Event ID | 2009 |
| Event name | tmnxSatSynclfTimRef1AlarmClear |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.9 |
| Default severity | cleared |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxHwIndex\$</i> , alarm <i>\$tmnxSatNotifySynclfTimRefAlarm\$</i> on reference 1 cleared |
| Cause | The tmnxSatSynclfTimRef1AlarmClear 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 tmnxSatSynclftimRef1Quality

Table 1306: tmnxSatSynclftimRef1Quality properties

| Property name | Value |
|----------------------------------|---|
| Application name | SATELLITE |
| Event ID | 2004 |
| Event name | tmnxSatSynclftimRef1Quality |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.4 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxSatId\$</i> , reference 1 received quality level <i>\$tmnxSatSynclftimingRef1RxQtyLvl\$</i> |
| Cause | The tmnxSatSynclftimRef1Quality 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 tmnxSatSynclftimRef2Alarm

Table 1307: tmnxSatSynclftimRef2Alarm properties

| Property name | Value |
|----------------------------------|---|
| Application name | SATELLITE |
| Event ID | 2010 |
| Event name | tmnxSatSynclftimRef2Alarm |
| 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 <i>\$tmnxHwIndex\$</i> , alarm <i>\$tmnxSatNotifySynclfTimRefAlarm\$</i> on reference 2 |
| Cause | The tmnxSatSynclfTimRef2Alarm 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 tmnxSatSynclfTimRef2AlarmClear

Table 1308: tmnxSatSynclfTimRef2AlarmClear properties

| Property name | Value |
|----------------------------------|---|
| Application name | SATELLITE |
| Event ID | 2011 |
| Event name | tmnxSatSynclfTimRef2AlarmClear |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.11 |
| Default severity | cleared |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxHwIndex\$</i> , alarm <i>\$tmnxSatNotifySynclfTimRefAlarm\$</i> on reference 2 cleared |
| Cause | The tmnxSatSynclfTimRef1AlarmClear 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 tmnxSatSynclfTimRef2Quality

Table 1309: *tmnxSatSynclfTimRef2Quality* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SATELLITE |
| Event ID | 2005 |
| Event name | tmnxSatSynclfTimRef2Quality |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.5 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxSatId\$</i> , reference 2 received quality level <i>\$tmnxSatSynclfTimingRef2RxQtyLvl\$</i> |
| Cause | The tmnxSatSynclfTimRef2Quality 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 tmnxSatSynclfTimRefSwitch

Table 1310: *tmnxSatSynclfTimRefSwitch* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SATELLITE |
| Event ID | 2002 |
| Event name | tmnxSatSynclfTimRefSwitch |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.2 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxSatId\$</i> , timing reference changed to <i>\$tmnxSatSynclfTimingRef1InUse\$</i> |

| Property name | Value |
|---------------|---|
| Cause | The tmnxSatSynclfTimRefSwitch 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 tmnxSatSynclfTimSystemQuality

Table 1311: tmnxSatSynclfTimSystemQuality properties

| Property name | Value |
|----------------------------------|---|
| Application name | SATELLITE |
| Event ID | 2003 |
| Event name | tmnxSatSynclfTimSystemQuality |
| SNMP notification prefix and OID | TIMETRA-SATELLITE-MIB.tmnxSatelliteNotifications.3 |
| Default severity | minor |
| Source stream | main |
| Message format string | Synchronous timing interface on satellite <i>\$tmnxSatId\$</i> , system quality level changed to <i>\$tmnxSatSynclfTimingSystemQltyLvI\$</i> |
| 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 1312: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1313: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1314: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> 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 tmnxPasswordAttemptsTime minutes. The value of the object tmnxPasswordAttemptsCount 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 open a CLI session. The value of the object tmnxSecNotifyAddrType 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 1315: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | A user access session ended. |
| Recovery | No recovery is required |

70.5 enable_admin

Table 1316: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1317: 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 | <i>\$appType\$</i> of <i>\$fileName\$</i> initiated by <i>\$userName\$</i> from <i>\$srcAddr\$</i> to <i>\$dstAddr\$</i> failed. |
| Cause | A FTP/TFTP transfer failed. |
| Effect | N/A |
| Recovery | No recovery is required |

70.7 ftp_transfer_successful

Table 1318: 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 | <i>\$appType\$</i> of <i>\$fileName\$</i> initiated by <i>\$userName\$</i> from <i>\$srcAddr\$</i> to <i>\$dstAddr\$</i> completed successfully. |
| Cause | A FTP/TFTP transfer completed successfully. |
| Effect | N/A |
| Recovery | No recovery is required |

70.8 ftp_user_login

Table 1319: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1320: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1321: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> 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 tmnxPasswordAttemptsTime minutes. The value of the object tmnxPasswordAttemptsCount 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 tmnxSecNotifyAddrType indicates the type of the IP address stored in the object tmnxSecNotifyAddr. The value of the object tmnxSecNotifyAddr indicates the IP address of the user attempting to connect via FTP. |
| Effect | The user is locked out for a period of tmnxPasswordAttemptsLockoutPeriod minutes. An FTP session is terminated. |
| Recovery | No recovery action is required. |

70.11 ftp_user_logout

Table 1322: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | The user access session ended. |
| Recovery | No recovery is required. |

70.12 grpc_auth

Table 1323: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 1324: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 1325: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1326: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1327: *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 <i>\$srcAddr\$</i> attempted more than <i>\$maxAttempts\$</i> 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 1328: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | The user access session ended. |
| Recovery | No recovery is required. |

70.18 host_snmp_attempts

Table 1329: *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 <i>\$hostAddress\$</i> is locked out for <i>\$lockoutTime\$</i> 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 1330: 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: <i>\$mafEntryDescription\$</i> .There have been <i>\$mafEntryDropped\$</i> matches since the previously logged match. Interface: <i>\$sourceInterface\$</i> , action: <i>\$mafEntryAction\$</i> <i>\$mafEntryProtocol\$</i> |
| 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 1331: 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: <ul style="list-style-type: none"> • User <i>\$userName\$</i> from <i>\$srcAddr\$</i> [session ID <i>\$sessionId\$</i>]: <i>\$command\$</i> • User <i>\$userName\$</i> from <i>\$srcAddr\$</i> [session ID <i>\$sessionId\$</i>]: <i>\$prompt\$ \$command\$</i> |
| 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 1332: 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: <ul style="list-style-type: none"> User <i>\$userName\$</i> from <i>\$srcAddr\$</i> [session ID <i>\$sessionId\$</i>]. Command not allowed for this user: <i>\$command\$</i> User <i>\$userName\$</i> from <i>\$srcAddr\$</i> [session ID <i>\$sessionId\$</i>]. Command not allowed for this user: <i>\$prompt\$ \$command\$</i> |
| 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 1333: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 1334: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> port <i>\$srcPort\$</i> to port <i>\$dstPort\$</i> session <i>\$sessionId\$</i> : <i>\$rpcName\$</i> 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 1335: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1336: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1337: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> 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 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 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 tmnxPasswordAttemptsLockoutPeriod minutes. A remote access session is terminated. |
| Recovery | No recovery action is required. |

70.27 netconf_user_logout

Table 1338: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | A user access session ended. |
| Recovery | No recovery is required |

70.28 radiusInetServerOperStatusChange

Table 1339: 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 <i>\$radiusServerInetAddress\$</i> operational status changed to <i>\$radiusServerOperStatus\$</i> . |
| 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 1340: 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 1341: 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 1342: 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 <i>\$attrType\$</i> ' <i>\$attrValue\$</i> ' received from RADIUS server for user ' <i>\$userName\$</i> ' |
| 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 1343: 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 \$sapDCpuProtPolicy\$. Policer=\$sapDcpFpProtocol\$(dynamic). Excd count=\$sapDcpFpDynExcdCount\$ |
| 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 1344: 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 \$sapEncapValue\$ on fp \$tmnxCardSlotNum\$/ \$tmnxFPNum\$ at \$sapDcpTimeEventOccured\$. 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 1345: 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 <i>\$sapDcpFpProtocol\$</i> policers freed for sap <i>\$sapEncapValue \$</i> on fp <i>\$tmnxCardSlotNum\$/ \$tmnxFPNum\$</i> at <i>\$sapDcpTimeEvent Occured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Excd count= <i>\$sapDcpFpDyn ExcdCount\$</i> |
| 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 1346: 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 1347: 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 <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Policer= <i>\$sapDcpFpProtocol\$(dynamic)</i> . Excd count= <i>\$sapDcpFpDynExcdCount\$</i> |
| 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::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 1348: 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 <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Policer= <i>\$sapDcpFpProtocol\$(dynamic)</i> . Excd count= <i>\$sapDcpFpDynExcdCount\$</i> |

| 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 1349: 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 <i>\$sapDcpFpLocMonPlcrName\$</i> for sap <i>\$sapEncap Value\$</i> on fp <i>\$tmnxCardSlotNum\$/ \$tmnxFPNum\$</i> detected as non-conformant at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProt Policy\$</i> . Excd count= <i>\$sapDcpFpLocMonExcdCount\$</i> |
| 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 1350: 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 <i>\$sapDcpFpLocMonPlcrName\$</i> for sap <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxFPNum\$</i> at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Excd count= <i>\$sapDcpFpLocMonExcdCount\$</i> |
| 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 1351: 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 <i>\$sapDcpFpLocMonPlcrName\$</i> for sap <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxFPNum\$</i> at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . |
| 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 1352: 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 <i>\$sapDcpFpLocMonPlcrName\$</i> for sap <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxFPNum\$</i> detected as non-conformant at <i>\$sapDcpTimeEventOccured\$</i> and cannot allocate |

| Property name | Value |
|---------------|---|
| | dynamic policers. Policy <i>\$sapDCpuProtPolicy\$</i> . Excd count= <i>\$sapDcpFpLocMonExcdCount\$</i> |
| 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 1353: 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 <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> newly conformant at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Policers= <i>\$sapDcpFpStaticPlcrName\$(static)</i> . Excd count= <i>\$sapDcpFpStaticExcdCount\$</i> |
| 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 1354: 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 <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum \$/tmnxFPNum\$</i> detected at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Policer= <i>\$sapDcpFpStaticPlcrName\$(static)</i> . Excd count= <i>\$sapDcpFpStaticExcdCount\$</i> |
| 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 1355: 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 <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCard SlotNum\$/\$tmnxFPNum\$</i> at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Policer= <i>\$sapDcpFpStaticPlcrName\$(static)</i> . Excd count= <i>\$sapDcpFpStaticExcdCount\$</i> |
| 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 1356: 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 <i>\$sapEncapValue\$</i> on fp <i>\$tmnxCardSlotNum \$/tmnxFPNum\$</i> at <i>\$sapDcpTimeEventOccured\$</i> . Policy <i>\$sapDCpuProtPolicy\$</i> . Policer= <i>\$sapDcpFpStaticPlcrName\$(static)</i> . Excd count= <i>\$sapDcpFpStaticExcdCount\$</i> |
| 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::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 1357: 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 <i>\$userName\$</i> and stored in <i>\$dstPath\$</i> |
| 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 1358: 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 <i>\$dstPath\$</i> |
| 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 1359: 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 <i>\$tmnxCpmFlashHwIndex\$</i> with operational status <i>\$tmnxCpmFlashOperStatus\$</i> . |
| 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 1360: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1361: 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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> 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 1362: 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 <i>\$tmnxSecNotifyUserName\$</i> from <i>\$tmnxSecNotifyAddr\$</i> attempted more than <i>\$tmnxPasswordAttemptsCount\$</i> times to log in, user locked out for <i>\$tmnxPasswordAttemptsLockoutPeriod\$</i> 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 tmnxPasswordAttemptsTime minutes. The value of the object tmnxPasswordAttemptsCount 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 <code>tmnxSecNotifyUserName</code> indicates the name of the user attempting to connect via SSH. The value of the object <code>tmnxSecNotifyAddrType</code> indicates the type of the IP address stored in the object <code>tmnxSecNotifyAddr</code> . The value of the object <code>tmnxSecNotifyAddr</code> indicates the IP address of the user attempting to connect via SSH. |
| Effect | The user is locked out for a period of <code>tmnxPasswordAttemptsLockoutPeriod</code> minutes. An SSH session is terminated. |
| Recovery | No recovery action is required. |

70.52 ssh_user_logout

Table 1363: 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 <code>\$userName\$</code> from <code>\$srcAddr\$</code> logged out |
| Cause | A user logged out. |
| Effect | The user access session ended. |
| Recovery | No recovery is required. |

70.53 sysDNSSecFailedAuthentication

Table 1364: 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 | <p>Possible messages:</p> <ul style="list-style-type: none"> 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 1365: 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 <i>\$tacPlusServerInetAddress\$</i> operational status changed to <i>\$tacplusServerOperStatus\$</i> . |
| 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 1366: *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 <i>\$tacplusOperStatus\$</i> . |
| 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 tacplusUserProfileInvalid

Table 1367: tacplusUserProfileInvalid properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2261 |
| Event name | tacplusUserProfileInvalid |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | security |
| Message format string | Invalid \$attrType\$ '\$attrValue\$' received from TACACS+ server for user '\$userName\$' |
| Cause | The TACACS+ server provided invalid user profile entry. |
| Effect | The TACACS+ user will not be authorized to execute any commands. |
| Recovery | The TACACS+ server configuration needs to be updated to contain only valid user profile entries. |

70.57 tmnxAppPkiCertVerificationFailed

Table 1368: 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. |

| Property name | Value |
|---------------|---|
| 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. |

70.58 tmnxCAProfileStateChange

Table 1369: 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 <i>\$tmnxPkiCAProfile\$</i> changed state to <i>\$tmnxPkiCAProfile OperState\$ \$tmnxSecNotifFailureReason\$</i> |
| 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. |

70.59 tmnxCAProfUpDueToRevokeChkCrIOpt

Table 1370: tmnxCAProfUpDueToRevokeChkCrIOpt properties

| Property name | Value |
|------------------|----------|
| Application name | SECURITY |

| Property name | Value |
|----------------------------------|---|
| Event ID | 2094 |
| Event name | tmnxCAProfUpDueToRevokeChkCrIOpt |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.27 |
| Default severity | minor |
| Source stream | security |
| Message format string | CA profile <i>\$tmnxPkiCAProfile\$</i> changed state to <i>\$tmnxPkiCAProfile OperState\$</i> regardless of <i>\$tmnxSecNotifFailureReason\$</i> due to crl-optional is set |
| Cause | The tmnxCAProfUpDueToRevokeChkCrIOpt 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. |

70.60 tmnxCertExport

Table 1371: 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 <i>\$tmnxSecNotifyImportExportType\$</i> input <i>\$tmnxSecNotifyUrl\$</i> output <i>\$tmnxSecNotifFile\$</i> format <i>\$tmnxSecNotifyImportExportFormat\$</i> : <i>\$tmnxSecEventOutcome\$</i> |

| Property name | Value |
|---------------|--|
| 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 |

70.61 tmnxCertImport

Table 1372: 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 <i>\$tmnxSecNotifyImportExportType\$</i> input <i>\$tmnxSecNotifyUrl\$</i> output <i>\$tmnxSecNotifFile\$</i> format <i>\$tmnxSecNotifyImportExportFormat\$</i> : <i>\$tmnxSecEventOutcome\$</i> |
| 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 |

70.62 tmnxCertKeyPairGen

Table 1373: *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: <ul style="list-style-type: none"> admin certificate gen-keypair <i>\$tmnxSecNotifyUrl\$</i> curve <i>\$tmnxSecNotifyCurve\$</i> : <i>\$tmnxSecEventOutcome\$</i> admin certificate gen-keypair <i>\$tmnxSecNotifyUrl\$</i> size <i>\$tmnxSecNotifyKeySize\$</i> type <i>\$tmnxSecNotifyKeyType\$</i> : <i>\$tmnxSecEventOutcome\$</i> |
| Cause | A tmnxCertKeyPairGen notification is generated when a user generates a cryptographic key with the admin certificate command |
| Effect | N/A |
| Recovery | N/A |

70.63 tmnxCliGroupSessionLimitExceeded

Table 1374: *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 |

| Property name | Value |
|-----------------------|---|
| Message format string | <i>\$tmnxSessionLimitExceededType\$</i> of CLI session group ' <i>\$tmnxSessionLimitExceededName\$</i> ' 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 tmnxSessionLimitExceededName indicates the name of the CLI session group 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 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 |

70.64 tmnxConfigCreate

Table 1375: tmnxConfigCreate properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2207 |
| Event name | tmnxConfigCreate |
| SNMP notification prefix and OID | TIMETRA-SYSTEM-MIB.tmnxSysNotifications.9 |
| Default severity | warning |
| Source stream | security |
| Message format string | <i>\$tmnxNotifyObjectName\$</i> 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 |

| Property name | Value |
|---------------|---|
| | 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. |

70.65 tmnxConfigDelete

Table 1376: 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 | <i>\$tmnxNotifyObjectName\$</i> 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 committed using model driven interfaces (for example, MD-CLI or NETCONF). |
| Effect | N/A |
| Recovery | No recovery is necessary. |

70.66 tmnxConfigModify

Table 1377: *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 | <i>\$tmnxNotifyObjectName\$</i> 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. |

70.67 tmnxCpmProtDefPolModified

Table 1378: *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 <i>\$tmnxCpmProtPolId\$</i> being modified by user. |

| Property name | Value |
|---------------|---|
| Cause | User modifies default access or default network policy. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

70.68 tmnxCpmProtExcdSapEcm

Table 1379: 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 <i>\$tmnxCpmProtExcdSapEcmOpCode\$</i> domain level <i>\$tmnxCpmProtExcdSapEcmLevel\$</i> MAC <i>\$tmnxCpmProtExcdSapEcmMac\$</i> SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| Cause | The tmnxCpmProtExcdSapEcm notification is generated when an Eth-CFM packet stream (identified by a source MAC address, domain level, and Eth-CFM opcode) arrives at a local SAP at a rate which exceeds the configured Eth-CFM rate limit for the stream. |
| Effect | One or more Eth-CFM packets arriving at the SAP was discarded. |
| Recovery | Reduce the packet transmission rate at the far end, or increase the locally configured Eth-CFM rate limit for the stream. |

70.69 tmnxCpmProtExcdSapIp

Table 1380: *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 <i>\$tmnxCpmProtExcdSapIpAddr\$</i> SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| Cause | The <i>tmnxCpmProtExcdSapIp</i> notification is generated when a source (identified by an IP address) sends a packet stream to a local SAP at a rate which exceeds the SAP's configured per-source-rate. [EFFECT] One or more packets arriving at the SAP was discarded. [RECOVERY] Reduce the packet transmission rate at the far end, OR increase the locally configured per-source-rate for the SAP, OR disable per-IP-source rate limiting on the SAP by setting TIMETRA-SAP-MIB::sapCpmProtMonitorIP to 'false'. |
| Effect | N/A |
| Recovery | N/A |

70.70 *tmnxCpmProtExcdSdpBind*

Table 1381: *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 |

| Property name | Value |
|-----------------------|--|
| Source stream | security |
| Message format string | Per-source packet arrival rate exceeded for MAC <i>\$tmnxCpmProtExcdSdpBindMac\$</i> SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| Cause | The <i>tmnxCpmProtExcdSdpBind</i> 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. |

70.71 *tmnxCpmProtExcdSdpBindEcm*

Table 1382: *tmnxCpmProtExcdSdpBindEcm* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2042 |
| Event name | <i>tmnxCpmProtExcdSdpBindEcm</i> |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB. <i>tmnxSecurityNotifications.15</i> |
| Default severity | warning |
| Source stream | security |
| Message format string | Eth-CFM packet arrival rate exceeded for Eth-CFM opcode <i>\$tmnxCpmProtExcdSdpBindEcmOpCode\$</i> domain level <i>\$tmnxCpmProtExcdSdpBindEcmLevel\$</i> MAC <i>\$tmnxCpmProtExcdSdpBindEcmMac\$</i> SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| Cause | The <i>tmnxCpmProtExcdSdpBindEcm</i> 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. |

| Property name | Value |
|---------------|---|
| 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. |

70.72 tmnxCpmProtExcdSdpBindIp

Table 1383: 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 <i>\$tmnxCpmProtExcdSdpBindIpAddr\$</i> SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| Cause | The tmnxCpmProtExcdSdpBindIp notification is generated when a source (identified by an IP address) sends a packet stream to a local mesh-sdp or spoke-sdp at a rate which exceeds the SDP's configured per-source-rate. |
| Effect | One or more packets arriving at the mesh-sdp or spoke-sdp was discarded. |
| Recovery | Reduce the packet transmission rate at the far end, or increase the locally configured per-source-rate for the SDP. |

70.73 tmnxCpmProtViolIf

Table 1384: *tmnxCpmProtViollf* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2030 |
| Event name | tmnxCpmProtViollf |
| 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 <i>\$vRtrIfIndex\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| 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 <i>tmnxCpmProtPolOverallRateLimit</i> of the interface protection policy specified by the managed object <i>TIMETRA-VRTR-MIB::vRtrIfCpmProtPolicyId</i> . Notifications are enabled if the value of the managed object <i>tmnxCpmProtPolAlarm</i> of the interface protection policy specified by the managed object <i>TIMETRA-VRTR-MIB::vRtrIfCpmProtPolicyId</i> is equal to 'true'. The notification may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the managed object <i>tmnxCpmProtPolOverallRateLimit</i> . Additional information can be retrieved in the SNMP table <i>tmnxCpmProtViollfTable</i> . |
| Effect | While the overall packet arrival rate limit is being exceeded, some protocol packets are dropped. |
| Recovery | No recovery is necessary. |

70.74 *tmnxCpmProtViollfOutProf*

Table 1385: *tmnxCpmProtViollfOutProf* properties

| Property name | Value |
|------------------|--------------------------|
| Application name | SECURITY |
| Event ID | 2085 |
| Event name | tmnxCpmProtViollfOutProf |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxCpmSecurityNotifications.22 |
| Default severity | warning |
| Source stream | security |
| Message format string | Out-of-Profile control packets rate exceeded for interface <i>\$vRtrIfIndex\$</i> . Hex Dump(First 64 bytes): <i>\$tmnCpmProtViolExcdPktHexDump\$</i> |
| Cause | The tmnCpmProtViolIfOutProf notification is generated when the rate at which incoming control packets are marked as out-of-profile specified by tmnCpmProtPolOutProfileRate is exceeded. This notification is generated when tmnCpmProtPolOutProfRateLogEvt 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, tmnCpmProtPolOutProfileRate for this interface. |

70.75 tmnCpmProtViolMac

Table 1386: tmnCpmProtViolMac properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2032 |
| Event name | tmnCpmProtViolMac |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxCpmSecurityNotifications.7 |
| Default severity | warning |
| Source stream | security |
| Message format string | Per-source packet arrival rate exceeded for MAC <i>\$tmnCpmProtViolMacAddress\$</i> SAP <i>\$sapEncapValue\$</i> in service <i>\$svcid\$</i> . Hex Dump(First 64 bytes): <i>\$tmnCpmProtViolExcdPktHexDump\$</i> |
| 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 tmnCpmProtPolPerSrcRateLimit of the SAP protection policy specified by the object TIMETRA-SAP-MIB::sapCpmProtPolicyId. Notifications are enabled if the value of the object tmnCpmProtPol |

| Property name | Value |
|---------------|---|
| | 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 tmnCpmProtPolPerSrcRateLimit. Additional information can be retrieved in the table tmnCpmProtExcdTable. |
| Effect | While the per-source rate limit is being exceeded, some protocol packets are dropped. |
| Recovery | No recovery is necessary. |

70.76 tmnCpmProtViolPort

Table 1387: tmnCpmProtViolPort properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2028 |
| Event name | tmnCpmProtViolPort |
| 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 <i>\$tmnxPortPortID</i> \$. Hex Dump(First 64 bytes): <i>\$tmnCpmProtViolExcdPktHexDump\$</i> |
| 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 tmnCpmProtLinkRateLimit. This event may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the managed object tmnCpmProtLinkRateLimit. Additional information can be retrieved from the SNMP table tmnCpmProtViolPortTable. |
| 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. |

70.77 tmnxCpmProtViolPortAgg

Table 1388: 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 <i>\$tmnxPortPortID\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| 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 tmnxCpmProtViolPortTable. |
| Effect | While the link-specific packet arrival rate limit is being exceeded, some protocol packets are dropped. |
| Recovery | No recovery is necessary. |

70.78 tmnxCpmProtViolSap

Table 1389: tmnxCpmProtViolSap properties

| Property name | Value |
|------------------|--------------------|
| Application name | SECURITY |
| Event ID | 2031 |
| Event name | tmnxCpmProtViolSap |

| Property name | Value |
|----------------------------------|---|
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump\$</i> |
| 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 <i>tmnxCpmProtPolOverallRateLimit</i> of the SAP protection policy specified by the object <i>TIMETRA-SAP-MIB::sapCpmProtPolicyId</i> . Notifications are enabled if the value of the object <i>tmnxCpmProtPolAlarm</i> of the SAP protection policy specified by the object <i>TIMETRA-SAP-MIB::sapCpmProtPolicyId</i> is equal to 'true'. The notification may indicate either a Denial-Of-Service Attack or an inappropriate configuration of the <i>tmnxCpmProtPolOverallRateLimit</i> . Additional information can be retrieved in the table <i>tmnxCpmProtViolSapTable</i> . |
| Effect | While the overall packet arrival rate limit is being exceeded, some protocol packets are dropped. |
| Recovery | No recovery is necessary. |

70.79 tmnxCpmProtViolSapOutProf

Table 1390: *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 |

| Property name | Value |
|-----------------------|---|
| Message format string | Out-of-Profile control packets rate exceeded for SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnCpmProtViolExcdPktHexDump\$</i> |
| Cause | The <i>tmnCpmProtViolSapOutProf</i> notification is generated when the rate at which incoming control packets are marked as out-of-profile specified by <i>tmnCpmProtPolOutProfileRate</i> is exceeded. This notification is generated when <i>tmnCpmProtPolOutProfRateLogEvtnt</i> 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, <i>tmnCpmProtPolOutProfileRate</i> for this SAP. |

70.80 tmnCpmProtViolSdpBind

Table 1391: *tmnCpmProtViolSdpBind* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2039 |
| Event name | <i>tmnCpmProtViolSdpBind</i> |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB. <i>tmnxSecurityNotifications.12</i> |
| Default severity | warning |
| Source stream | security |
| Message format string | Overall packet arrival rate exceeded for SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnCpmProtViolExcdPktHexDump\$</i> |
| Cause | The <i>tmnCpmProtViolSdpBind</i> 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. |

70.81 tmnCpmProtViolSdpBindOutProf

Table 1392: tmnCpmProtViolSdpBindOutProf properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2089 |
| Event name | tmnCpmProtViolSdpBindOutProf |
| 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnCpmProtViolExcdPktHexDump\$</i> |
| Cause | The tmnCpmProtViolSdpBindOutProf notification is generated when the rate at which incoming control packets are marked as out-of-profile specified by tmnCpmProtPolOutProfileRate is exceeded. This notification is generated when tmnCpmProtPolOutProfRateLogEvt 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, tmnCpmProtPolOutProfileRate for this SDP binding. |

70.82 tmnCpmProtViolVdoSvcClient

Table 1393: tmnCpmProtViolVdoSvcClient properties

| Property name | Value |
|------------------|----------------------------|
| Application name | SECURITY |
| Event ID | 2033 |
| Event name | tmnCpmProtViolVdoSvcClient |

| Property name | Value |
|----------------------------------|---|
| 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 <i>\$tmnxCpmProtViolVdoSvc CltAddr\$</i> in service <i>\$svclId\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProt ViolExcdPktHexDump\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

70.83 tmnxCpmProtViolVdoVrtrClient

Table 1394: *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 |
| Message format string | Per-source rate limit exceeded for source <i>\$tmnxCpmProtViolVdoVrtrCl tAddr\$</i> . Hex Dump(First 64 bytes): <i>\$tmnxCpmProtViolExcdPktHexDump \$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

70.84 tmnxDcpCardFpEventOvrflw

Table 1395: 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. |

70.85 tmnxDcpCardFpEventOvrflwClr

Table 1396: 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 |

| Property name | Value |
|-----------------------|--|
| Message format string | <i>\$tmnxDcpMissingNotificationCount\$</i> Distributed CPU Protection FP log events were dropped in the last event throttling interval on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxDcpTimeEventOccured\$</i> |
| Cause | The <i>tmnxDcpCardFpEventOvrflwClr</i> 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. |

70.86 tmnxDcpCardSapEventOvrflw

Table 1397: *tmnxDcpCardSapEventOvrflw* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2081 |
| Event name | <i>tmnxDcpCardSapEventOvrflw</i> |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB. <i>tmnxChassisNotification.73</i> |
| Default severity | warning |
| Source stream | security |
| Message format string | Distributed CPU Protection SAP log event overflow occurred on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxDcpTimeEventOccured\$</i> |
| Cause | The <i>tmnxDcpCardSapEventOvrflw</i> 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. |

70.87 tmnxDcpCardSapEventOvrflwClr

Table 1398: *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 | <i>\$tmnxDcpMissingNotificationCount\$</i> Distributed CPU Protection SAP log events were dropped in the last event throttling interval on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxDcpTimeEventOccured\$</i> |
| 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. |

70.88 tmnxDcpCardVrtrlfEventOvrflw

Table 1399: *tmnxDcpCardVrtrlfEventOvrflw* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2082 |
| Event name | tmnxDcpCardVrtrlfEventOvrflw |
| 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 <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxDcpTimeEventOccured\$</i> |

| Property name | Value |
|---------------|--|
| Cause | The tmnxDcpCardVrtrlfEventOvrflw 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. |

70.89 tmnxDcpCardVrtrlfEventOvrflwClr

Table 1400: tmnxDcpCardVrtrlfEventOvrflwClr properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2051 |
| Event name | tmnxDcpCardVrtrlfEventOvrflwClr |
| SNMP notification prefix and OID | TIMETRA-CHASSIS-MIB.tmnxChassisNotification.79 |
| Default severity | warning |
| Source stream | security |
| Message format string | <i>\$tmnxDcpMissingNotificationCount\$</i> Distributed CPU Protection Netwk_if log events were dropped in the last event throttling interval on card <i>\$tmnxChassisNotifyCardSlotNum\$</i> at <i>\$tmnxDcpTimeEvent Occured\$</i> |
| Cause | The tmnxDcpCardVrtrlfEventOvrflwClr 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. |

70.90 tmnxDcpFpDynPoolUsageHiAlmClear

Table 1401: *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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxFPNum\$</i> at <i>\$tmnxDcpTimeEventOccured\$</i> |
| 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. |

70.91 tmnxDcpFpDynPoolUsageHiAlmRaise

Table 1402: *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 <i>\$tmnxCardSlotNum\$</i> / <i>\$tmnxFPNum\$</i> at <i>\$tmnxDcpTimeEventOccured\$</i> |

| Property name | Value |
|---------------|--|
| 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. |

70.92 tmnxFileCopied

Table 1403: 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 <i>\$tmnxSecNotifyUrl\$</i> copy to <i>\$tmnxSecNotifyNewUrl\$</i> : <i>\$tmnxSecEventOutcome\$</i> |
| Cause | A tmnxFileCopied notification is generated when a user copies a file through the file command |
| Effect | N/A |
| Recovery | N/A |

70.93 tmnxFileDeleted

Table 1404: *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 <i>\$tmnxSecNotifyUrl\$</i> delete : <i>\$tmnxSecEventOutcome\$</i> |
| Cause | A <i>tmnxFileDeleted</i> notification is generated when a user deletes a file through the file command |
| Effect | N/A |
| Recovery | N/A |

70.94 *tmnxFileMoved*

Table 1405: *tmnxFileMoved* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2235 |
| Event name | tmnxFileMoved |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.60 |
| Default severity | minor |
| Source stream | security |
| Message format string | File <i>\$tmnxSecNotifyUrl\$</i> move to <i>\$tmnxSecNotifyNewUrl\$</i> : <i>\$tmnxSecEventOutcome\$</i> |
| Cause | A <i>tmnxFileMoved</i> notification is generated when a user moves a file through the file command |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

70.95 tmnxFileUnzip

Table 1406: 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 <i>\$tmnxSecNotifyUrl\$</i> destination <i>\$tmnxSecNotifyDestUrl\$</i> and result <i>\$tmnxSecNotifFileUnzipResult\$</i> |
| 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 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. |

70.96 tmnxKeyChainAuthFailure

Table 1407: *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 <i>\$tmnxKeyChainAuthAddress\$</i> virtual router <i>\$vRtrID\$</i> dropped due to key chain authentication failure and possible reason is <i>\$tmnxKeyChainAuthFailReason\$</i> . |
| 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. |

70.97 tmnxMD5AuthFailure

Table 1408: *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 |

| Property name | Value |
|-----------------------|---|
| Message format string | Incoming packet from source address <i>\$tmnxMD5AuthAddr\$</i> virtual router <i>\$vRtrID\$</i> dropped due to MD5 authentication failure and possible reason is <i>\$tmnxMD5AuthFailReason\$</i> . |
| 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. |

70.98 tmnxPasswordHashingChanged

Table 1409: *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 <i>\$tmnxSecNotifOldPasswordHashing\$</i> to <i>\$tmnxSecNotifNewPasswordHashing\$</i> |
| Cause | The <i>tmnxPasswordHashingChanged</i> notification is generated upon the change of password hashing algorithm (<i>tmnxPasswordHashing</i>). The value of the object <i>tmnxSecNotifNewPasswordHashing</i> indicates the new password hashing algorithm. The value of the object <i>tmnxSecNotifOldPasswordHashing</i> 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 <i>tmnxPasswordHashing</i> . |
| Recovery | No recovery action is required. |

70.99 tmnxPkiCAProfActnStatusChg

Table 1410: 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 | <i>\$tmnxPkiCAProfActnType\$</i> for ca-profile (<i>\$tmnxPkiCAProfile\$</i>) <i>\$tmnxPkiCAProfActnStatus\$</i> . ca-response: <i>\$tmnxCAProfActnStatusCode\$</i> . <i>\$tmnxPkiCAProfActnStatusString\$</i> |
| Cause | The tmnxPkiCAProfActnStatusChg notification is generated when tmnxPkiCAProfActnStatus changes status. More information is available through tmnxPkiCAProfActnStatusString and tmnxPkiCAProfActnStatusCode. |
| Effect | This is due to the action performed using tmnxPkiCAProfActnTable. |
| Recovery | Depending on the information available in this trap, another tmnxPkiCAProfActnType request may be issued by correcting the parameters in the tmnxPkiCAProfActnTable. |

70.100 tmnxPkiCAProfCrlUpdAllUrlsFail

Table 1411: tmnxPkiCAProfCrlUpdAllUrlsFail properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2108 |
| Event name | tmnxPkiCAProfCrlUpdAllUrlsFail |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.40 |

| Property name | Value |
|-----------------------|---|
| Default severity | minor |
| Source stream | security |
| Message format string | Failed to update the CRL file from <i>\$tmnxPkiCAProfUrl\$</i> (<i>\$tmnxPkiCAProfUrlId\$</i>), the last of all the URLs for CA profile <i>\$tmnxPkiCAProfile\$</i> , due to <i>\$tmnxSecNotifFailureReason\$</i> |
| Cause | A <i>tmnxPkiCAProfCrlUpdAllUrlsFail</i> notification is generated when the CRL update operation failed after attempting all URLs for an existing CA Profile. The CA Profile is configured via <i>tmnxPkiCAProfileTable</i> . URLs for an existing CA Profile are configured via <i>tmnxPkiCAProfUrlTable</i> . |
| Effect | When <i>tmnxPkiCAProfAtCrlUpdScheduleT</i> is 'nextUpdateBased (1)' and <i>tmnxPkiCAProfAtCrlUpdRetryIntv</i> 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) <i>tmnxPkiCAProfAtCrlUpdRetryIntv</i> (>0) seconds, when <i>tmnxPkiCAProfAtCrlUpdScheduleT</i> is 'nextUpdateBased (1)', or 2) <i>tmnxPkiCAProfAtCrlUpdPrdcUpdIntv</i> seconds, when <i>tmnxPkiCAProfAtCrlUpdScheduleT</i> is 'periodic (2)'. |
| Recovery | Make sure the URLs specified in <i>tmnxPkiCAProfUrlTable</i> are correct. |

70.101 tmnxPkiCAProfCrlUpdateStart

Table 1412: *tmnxPkiCAProfCrlUpdateStart* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2105 |
| Event name | <i>tmnxPkiCAProfCrlUpdateStart</i> |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB. <i>tmnxSecurityNotifications.37</i> |
| Default severity | minor |
| Source stream | security |
| Message format string | Started updating the CRL file for CA profile <i>\$tmnxPkiCAProfileNameForNotify\$</i> |

| Property name | Value |
|---------------|--|
| 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. |

70.102 tmnxPkiCAProfCrlUpdateSuccess

Table 1413: 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 <i>\$tmnxPkiCAProfUrl\$</i> (<i>\$tmnxPkiCAProfUrlId\$</i>) for CA profile <i>\$tmnxPkiCAProfile\$</i> |
| 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 tmnxPkiCAProfAtCrlUpdScheduleT. |
| Recovery | No recovery is required for this notification. |

70.103 tmnxPkiCAProfCrlUpdateUrlFail

Table 1414: *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 <i>\$tmnxPkiCAProfUrl\$</i> (<i>\$tmnxPkiCAProfUrlId\$</i>) due to <i>\$tmnxSecNotifFailureReason\$</i> |
| Cause | A <i>tmnxPkiCAProfCrlUpdateUrlFail</i> 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 <i>tmnxPkiCAProfileTable</i> . URLs for an existing CA Profile are configured via <i>tmnxPkiCAProfUrlTable</i> . A <i>tmnxPkiCAProfCrlUpdateUrlFail</i> will not be sent when the URL is the last one in the URL list for an existing CA Profile. In such case, a <i>tmnxPkiCAProfCrlUpdAllUrlsFail</i> 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 <i>tmnxPkiCAProfUrlTable</i> are correct. |

70.104 *tmnxPkiCAProfCrlUpdLargPreUpdTm*

Table 1415: *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 |

| Property name | Value |
|-----------------------|--|
| Source stream | security |
| Message format string | The CRL pre-update time for CA profile <i>\$tmnxPkiCAProfileNameForNotify\$</i> might be too large |
| Cause | A <i>tmnxPkiCAProfCrlUpdLargPreUpdTm</i> 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 <i>tmnxPkiCAProfAtCrlUpdAdminState</i> to 'inService (2)' plus the pre-update time. The last successful update time is stored in <i>tmnxPkiCAProfAtCrlUpdLstSucsTmSt</i> . The pre-update time is configured via <i>tmnxPkiCAProfAtCrlUpdPreUpdTime</i> . |
| Effect | The system will update the CRL again in <i>tmnxPkiCAProfAtCrlUpdRetryIntv</i> seconds rather than immediately. |
| Recovery | Configure <i>tmnxPkiCAProfAtCrlUpdPreUpdTime</i> 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 <i>tmnxPkiCAProfAtCrlUpdAdminState</i> to 'inService (2)'. No recovery is needed for if the notification is generated in case of setting <i>tmnxPkiCAProfAtCrlUpdAdminState</i> to 'inService (2)'. |

70.105 *tmnxPkiCAProfCrlUpdNoNxtUpdTime*

Table 1416: *tmnxPkiCAProfCrlUpdNoNxtUpdTime* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2110 |
| Event name | <i>tmnxPkiCAProfCrlUpdNoNxtUpdTime</i> |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB. <i>tmnxSecurityNotifications.42</i> |
| Default severity | minor |
| Source stream | security |
| Message format string | No further scheduled CRL update for CA profile <i>\$tmnxPkiCAProfileNameForNotify\$</i> 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 |

| Property name | Value |
|---------------|--|
| Cause | A tmnxPkiCAProfCrIUpdNoNxtUpdTime notification is generated when tmnxPkiCAProfAtCrIUpdScheduleT 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) tmnxPkiCAProfAtCrIUpdRetryIntv 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 tmnxPkiCAProfAtCrIUpdScheduleT to 'periodic (2)' if the system is to check for an updated CRL every tmnxPkiCAProfAtCrIUpdPrdcUpdIntv seconds. Otherwise, configure the tmnxPkiCAProfAtCrIUpdAdminState to 'outOfService (3)'. |

70.106 tmnxPkiCAProfRevokeChkWarning

Table 1417: tmnxPkiCAProfRevokeChkWarning properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2093 |
| Event name | tmnxPkiCAProfRevokeChkWarning |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | security |
| Message format string | <i>\$tmnxSecNotifTunnelName\$</i> : CRL check skipped for <i>\$skippedCert\$</i> issued by ca-profile <i>\$tmnxPkiCAProfile\$</i> while verifying EE cert <i>\$ee CertSubject\$</i> due to <i>\$tmnxSecNotifFailureReason\$</i> |
| 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. |

70.107 tmnxPkiCertAfterExpWarning

Table 1418: 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 <i>\$tmnxSecNotifFile\$</i> used by <i>\$tmnxSecNotifClientAppName\$</i> 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. |

70.108 tmnxPkiCertBeforeExpWarning

Table 1419: 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 |

| Property name | Value |
|-----------------------|--|
| Message format string | Certificate <i>\$tmnxSecNotifFile\$</i> used by <i>\$tmnxSecNotifClientAppName\$</i> will expire in <i>\$tmnxPkiExpRemainingHours\$</i> hour(s) and <i>\$tmnxPkiExpRemainingMinutes\$</i> minute(s). |
| Cause | The tmnxPkiCertBeforeExpWarning notification is generated when the certificate indicated in tmnxSecNotifFile will expire in the time period indicated by tmnxPkiExpRemainingHours and tmnxPkiExpRemaining Minutes. |
| Effect | The indicated certificate will expire. |
| Recovery | Replace the indicated file with an updated certificate. |

70.109 tmnxPkiCertChainCompareCaNoMatch

Table 1420: 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 |
| Source stream | main |
| Message format string | Compute chain for certificate file ' <i>\$tmnxPkiCertFileNameNotif\$</i> ': No chain contains certificate with subject DN ' <i>\$tmnxPkiCertSubjectNotif\$</i> ', serial ' <i>\$tmnxPkiCertSerialNumberNotif\$</i> '. 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). |

70.110 tmnxPkiCertExpWarningCleared

Table 1421: 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 <i>\$tmnxSecNotifFile\$</i> used by <i>\$tmnxSecNotifClientAppName\$</i> is no longer applicable because of the following reason: <i>\$tmnxPkiExpReason\$</i> . |
| 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. |

70.111 tmnxPkiCertNotYetValid

Table 1422: 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 |

| Property name | Value |
|-----------------------|--|
| Source stream | security |
| Message format string | Certificate <i>\$tmnxSecNotifFile\$</i> used by <i>\$tmnxSecNotifClientAppName\$</i> 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. |

70.112 tmnxPkiCertUpdUpdateFailed

Table 1423: tmnxPkiCertUpdUpdateFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2247 |
| Event name | tmnxPkiCertUpdUpdateFailed |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.72 |
| Default severity | minor |
| Source stream | security |
| Message format string | Certificate file: <i>\$tmnxPkiCertUpdCertFileNameNotif\$</i> - Update failed - Reason: <i>\$tmnxPkiCertUpdFailureReasonNotif\$</i> |
| 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. |

70.113 tmnxPkiCertUpdUpdateFinished

Table 1424: 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: <i>\$tmnxPkiCertUpdCertFileNameNotif\$</i> - Update finished - Serial number: <i>\$tmnxPkiCertUpdSerialNumberNotif\$</i> - Subject: <i>\$tmnxPkiCertUpdSubjectNotif\$</i> |
| 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. |

70.114 tmnxPkiCertUpdUpdateStarted

Table 1425: 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 |

| Property name | Value |
|-----------------------|--|
| Source stream | security |
| Message format string | Certificate file: <i>\$tmnxPkiCertUpdCertFileNameNotif\$</i> - 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. |

70.115 tmnxPkiCertVerificationFailed

Table 1426: 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 <i>\$tmnxSecNotifTunnelName\$</i> : Certificate <i>\$tmnxSecNotifCert\$</i> verification failed due to <i>\$tmnxSecNotifFailureReason\$</i> |
| 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. |

70.116 tmnxPkiCRLAfterExpWarning

Table 1427: *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 <i>\$tmnxSecNotifFile\$</i> 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). |

70.117 tmnxPkiCRLBeforeExpWarning

Table 1428: *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 <i>\$tmnxSecNotifFile\$</i> will expire in <i>\$tmnxPkiExpRemainingHours\$</i> hour(s) and <i>\$tmnxPkiExpRemainingMinutes\$</i> minute(s). |
| Cause | The tmnxPkiCRLBeforeExpWarning notification is generated when the CRL (certificate revocation list) indicated in tmnxSecNotifFile will expire |

| Property name | Value |
|---------------|--|
| | in the time period indicated by tmnxPkiExpRemainingHours and tmnxPkiExpRemainingMinutes. |
| Effect | The indicated CRL (certificate revocation list) will expire. |
| Recovery | Replace the indicated file with an updated CRL (certificate revocation list). |

70.118 tmnxPkiCRLExpWarningCleared

Table 1429: 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 <i>\$tmnxSecNotifFile\$</i> is no longer applicable because of the following reason: <i>\$tmnxPkiExpReason\$</i> |
| 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. |

70.119 tmnxPkiCRLNotYetValid

Table 1430: *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 <i>\$tmnxSecNotifFile\$</i> 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 'crIOptional (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. |

70.120 tmnxPkiFileReadFailed

Table 1431: *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 |

| Property name | Value |
|-----------------------|---|
| Message format string | File <i>\$tmnxSecNotifFile\$</i> read failed due to <i>\$tmnxSecNotifFailureReason\$</i> |
| Cause | The tmnxPkiFileReadFailed notification is generated when an attempt to read the file fails. Reason of the failure is indicated by the tmnxSecNotifFailureReason 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. |

70.121 tmnxPkiFileWriteFailed

Table 1432: 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 |
| Source stream | security |
| Message format string | File <i>\$tmnxSecNotifFile\$</i> write failed due to <i>\$tmnxSecNotifFailureReason\$</i> |
| Cause | The tmnxPkiFileWriteFailed notification is generated when an attempt to write the file fails. Reason for the failure is indicated by the tmnxSecNotifFailureReason 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. |

70.122 tmnxSecComputeCertChainFailure

Table 1433: 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 <i>\$tmnxSecNotifFile\$</i> is incomplete due to <i>\$tmnxSecNotifFailureReason\$</i> |
| 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. |

70.123 tmnxSecNotifFileReloaded

Table 1434: 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 |

| Property name | Value |
|-----------------------|--|
| Source stream | security |
| Message format string | <i>\$tmnxSecNotifFileType\$</i> file " <i>\$tmnxSecNotifFile\$</i> " has been reloaded. |
| Cause | The tmnxSecNotifFileReloaded notification is generated when the certificate or key indicated in tmnxSecNotifFile is reloaded. tmnxSecNotifFileType indicates whether a certificate or key has been reloaded. |
| Effect | The indicated certificate or key has been reloaded. |
| Recovery | None needed. |

70.124 tmnxSecNotifKeyChainExpired

Table 1435: 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 |
| Message format string | Keychain <i>\$tmnxKeyChainName\$</i> : last entry has expired; called by <i>\$tmnxSecNotifOrigProtocol\$</i> |
| 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 |

70.125 tmnxSecPwdHistoryFileLoadFailed

Table 1436: *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 tmnxSecPwdHistLoadFailReason is set to 'notFound(1)', a new, empty history file will be created. |
| Recovery | Investigation might be warranted. |

70.126 tmnxSecPwdHistoryFileWriteFailed

Table 1437: *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 |

| Property name | Value |
|-----------------------|--|
| 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. |

70.127 tmnxSecSignedSwCpmBootEvent

Table 1438: 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 |
| Source stream | main |
| Message format string | CPM <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> has booted with a secure-boot status of <i>\$tmnxCpmSecureBootEnabled\$</i> |
| 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. |

70.128 tmnxSecSignedSwImgValFail

Table 1439: *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 <i>\$tmnxSecureBootValdImgUrl\$</i> , for CPM <i>\$tmnxChassisNotifyCpmCardSlotNum\$</i> , failed to be validated. As a result, the CPM will not boot |
| Cause | The <i>tmnxSecSignedSwImgValFail</i> 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. |

70.129 *tmnxSSHInvalidPacketLength*

Table 1440: *tmnxSSHInvalidPacketLength* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2262 |
| Event name | tmnxSSHInvalidPacketLength |
| SNMP notification prefix and OID | TIMETRA-SECURITY-MIB.tmnxSecurityNotifications.81 |
| Default severity | minor |
| Source stream | security |

| Property name | Value |
|-----------------------|---|
| Message format string | SSH connection ID \$tmnxUserConnectionId from source \$tmnxSecNotifyAddr discarded a packet with length \$tmnxSSHPacketLength bytes with reason 'wrong-packet-length' |
| Cause | The tmnxSSHInvalidPacketLength notification is generated when an SSH packet with an invalid length is received either by an SSH client or an SSH server. On server side the value of the object tmnxUserConnectionId indicates the ID of the SSH connection. On client side the value of tmnxUserConnectionId is set to 0. 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 source IP address of the remote SSH peer. The value of the object tmnxSSHPacketLength indicates the length expressed in bytes of the received SSH packet. |
| Effect | The packet is discarded and the SSH connection may be terminated. |
| Recovery | No recovery action is required. |

70.130 tmnxSSHListeningPortChanged

Table 1441: 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. |

70.131 tmnxSSHListeningPortInUse

Table 1442: 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 |
| 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. |

70.132 tmnxSSHListeningPortOccupied

Table 1443: 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 |

| Property name | Value |
|-----------------------|---|
| Source stream | main |
| Message format string | SSH port <i>\$tmnxSSHListeningPort\$</i> cannot be configured because this port is used by another application |
| Cause | The <i>tmnxSSHListeningPortOccupied</i> 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. |

70.133 tmnxSSHSessionFailed

Table 1444: *tmnxSSHSessionFailed* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2240 |
| Event name | <i>tmnxSSHSessionFailed</i> |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | security |
| Message format string | SSH session failed from client <i>\$tmnxSecNotifyAddr\$</i> , reason ' <i>\$tmnxSecSSHSessionFailedReason\$</i> ' |
| Cause | The <i>tmnxSSHSessionFailed</i> notification is generated upon the failure of an SSH session establishment. The value of the object <i>tmnxSecNotifyAddrType</i> indicates the type of the IP address stored in the object <i>tmnxSecNotifyAddr</i> . The value of the object <i>tmnxSecNotifyAddr</i> indicates the source IP address of the user attempting to establish the SSH session. The value of the object <i>tmnxSecSSHSessionFailedReason</i> indicates the reason of the establishment failure. |
| Effect | SSH session is not established and connection is closed. |
| Recovery | No recovery action is required. |

70.134 tmnxStateChange

Table 1445: 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 |
| Message format string | Status of <i>\$tmnxNotifyObjectName\$</i> changed administrative state: <i>\$tmnxNotifyRowAdminState\$</i> , operational state: <i>\$tmnxNotifyRowOperState\$</i> |
| 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. |

70.135 tmnxSysAppLicenseInsufficient

Table 1446: 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 |

| Property name | Value |
|-----------------------|---|
| Message format string | License <i>\$tmnxSysAppLicenseState\$</i> for <i>\$tmnxSysLicensingNotifyGroup\$</i> feature ' <i>\$tmnxSysLicensedNotifyAppName\$</i> ': <i>\$tmnxSysLicenseErrorReason\$</i> |
| Cause | The <i>tmnxSysAppLicenseInsufficient</i> notification is generated periodically when licensing for an application is detected to be insufficient. The details of the error is specified in <i>tmnxSysLicenseErrorReason</i> . 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. |

70.136 *tmnxSysLicenseActivated*

Table 1447: *tmnxSysLicenseActivated* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2125 |
| Event name | <i>tmnxSysLicenseActivated</i> |
| SNMP notification prefix and OID | TIMETRA-SYSTEM-MIB. <i>tmnxSysNotifications.75</i> |
| Default severity | warning |
| Source stream | security |
| Message format string | <i>\$tmnxHwIndex\$</i> is running with a valid license. |
| Cause | The <i>tmnxSysLicenseActivated</i> notification is generated each time a license is activated on the system. |
| Effect | The system is running with the license specified in <i>tmnxSysLicenseName</i> . |
| Recovery | No recovery. |

70.137 tmnxSysLicenseCleared

Table 1448: 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 | <i>\$tmnxHwIndex\$</i> is no longer running with a license. |
| 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. |

70.138 tmnxSysLicenseExpiresSoon

Table 1449: 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 <i>\$tmnxHwIndex\$</i> expires <i>\$tmnxSysLicenseTimeLeft\$</i> . |

| Property name | Value |
|---------------|--|
| 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. |

70.139 tmnxSysLicenseInvalid

Table 1450: tmnxSysLicenseInvalid properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2091 |
| Event name | tmnxSysLicenseInvalid |
| SNMP notification prefix and OID | TIMETRA-SYSTEM-MIB.tmnxSysNotifications.59 |
| Default severity | major |
| Source stream | security |
| Message format string | Error - <i>\$tmnxSysLicenseErrorReason\$</i> record. <i>\$tmnxHwIndex\$</i> will <i>\$tmnxSysLicenseErrorAction\$</i> <i>\$tmnxSysLicenseTimeLeft\$</i> . |
| 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. |

70.140 tmnxSysLicenseUpdateRequired

Table 1451: *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. |
| Recovery | Update and activate the updated license. |

70.141 tmnxSysLicenseValid

Table 1452: *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 | <i>\$tmnxHwIndex\$</i> 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. |

| Property name | Value |
|---------------|--|
| Effect | The system is running with the license specified in tmnxSysLicense Name. |
| Recovery | No recovery. |

70.142 tmnxSysLicensingStateOk

Table 1453: tmnxSysLicensingStateOk properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2250 |
| Event name | tmnxSysLicensingStateOk |
| SNMP notification prefix and OID | TIMETRA-SYSTEM-MIB.tmnxSysNotifications.96 |
| Default severity | warning |
| Source stream | security |
| Message format string | <i>\$tmnxHwIndex\$</i> 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. |

70.143 tmnxSysStandbyLicensingError

Table 1454: tmnxSysStandbyLicensingError properties

| Property name | Value |
|------------------|------------------------------|
| Application name | SECURITY |
| Event ID | 2221 |
| Event name | tmnxSysStandbyLicensingError |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-SYSTEM-MIB.tmnxSysNotifications.76 |
| Default severity | major |
| Source stream | main |
| Message format string | <i>\$tmnxHwIndex\$</i> is not licensed. <i>\$tmnxSysLicenseErrorReason\$</i> . |
| 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. |

70.144 tmnxSysStandbyLicensingReady

Table 1455: *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 | <i>\$tmnxHwIndex\$</i> 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. |

70.145 tmnxSysSwDSValidationResult

Table 1456: *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 |
| Message format string | Software location <i>\$tmnxSysSwDSValidationIndex\$</i> at <i>\$tmnxSysSwDSValidationUrl\$</i> digital signature state is <i>\$tmnxSysSwDSValidationState\$</i> . |
| Cause | A software digital signature validation has completed. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

70.146 tmnxSystemPasswordChangedByAdmin

Table 1457: *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 |

| Property name | Value |
|-----------------------|---|
| Message format string | User '\$tmnxSecNotifyAdminUserName\$' changed the local system ' '\$tmnxSecNotifyLocalSystemPassword\$' |
| Cause | The tmnxSystemPasswordChangedByAdmin notification is generated upon the change of an administrative password by a user with administrative rights. The value of the object tmnxSecNotifyAdmin UserName indicates the user name who changed the password. The value of the object tmnxSecNotifyLocalSystemPassword indicates the administrative password that was changed. |
| Effect | Users with administrative rights will be able to authenticate with the new password only. |
| Recovery | No recovery action is required. |

70.147 tmnxTelnetListeningPortChanged

Table 1458: 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 '\$tmnxTelnetListeningPort\$' |
| 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. |

70.148 tmnxTelnetListeningPortInUse

Table 1459: 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 |
| Message format string | Application is trying to open a connection on Telnet port <i>\$tmnxTelnetListeningPort\$</i> |
| 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. |

70.149 tmnxTelnetListeningPortOccupied

Table 1460: 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 |

| Property name | Value |
|-----------------------|---|
| Source stream | main |
| Message format string | Telnet port <i>\$tmnxTelnetListeningPort\$</i> cannot be configured because this port is used by another application |
| Cause | The <i>tmnxTelnetListeningPortOccupied</i> 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. |

70.150 tmnxUserPasswordChangedByAdmin

Table 1461: *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 ' <i>\$tmnxSecNotifyAdminUserName\$</i> ' changed the password for user ' <i>\$tmnxSecNotifyLocalUserName\$</i> ' |
| Cause | The <i>tmnxUserPasswordChangedByAdmin</i> notification is generated upon the change of a password of a local user by a user with administrative rights. The value of the object <i>tmnxSecNotifyLocalUserName</i> indicates the user name for which the password has been changed. The value of the object <i>tmnxSecNotifyAdminUserName</i> 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. |

70.151 tmnxUsrProfSessionLimitExceeded

Table 1462: 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 |
| Message format string | <i>\$tmnxSessionLimitExceededType\$</i> of user profile ' <i>\$tmnxSessionLimitExceededName\$</i> ' 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) |

70.152 tSecSgndSwUefiVarsUpdtReqd

Table 1463: *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 <i>\$tmnxChassisNotifyCpmCard SlotNum\$</i> |
| 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. |
| 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. |

70.153 user_disconnect

Table 1464: *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 <i>\$userName\$</i> from <i>\$srcAddr\$</i> logged out by <i>\$disconnectedBy\$</i> |

| Property name | Value |
|---------------|---|
| Cause | A user was logged out by the administrator. |
| Effect | The user's console/telnet/ftp session terminated. |
| Recovery | No recovery is required |

70.154 vRtrIfDcpDynamicConform

Table 1465: vRtrIfDcpDynamicConform properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2073 |
| Event name | vRtrIfDcpDynamicConform |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.54 |
| Default severity | warning |
| Source stream | security |
| Message format string | Network_if \$vRtrIfIndex\$ on fp \$tmnxCardSlotNum\$/ \$tmnxFPNum \$ newly conformant at \$vRtrIfDcpTimeEventOccured\$. Policy \$vRtrIfDcpCpuProtPolicy\$. 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. |

70.155 vRtrIfDcpDynamicEnforceAlloc

Table 1466: 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 |
| Message format string | Dynamic \$vRtrIfDcpFpProtocol\$ policers allocated for network_if \$vRtrIfIndex\$ on fp \$tmnxCardSlotNum\$/\$tmnxFPNum\$ at \$vRtrIfDcpTimeEventOccured\$. Policy \$vRtrIfDcpProtPolicy\$. |
| 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. |

70.156 vRtrIfDcpDynamicEnforceFreed

Table 1467: vRtrIfDcpDynamicEnforceFreed properties

| Property name | Value |
|------------------|----------|
| Application name | SECURITY |
| Event ID | 2079 |

| Property name | Value |
|----------------------------------|---|
| Event name | vRtrIfDcpDynamicEnforceFreed |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.60 |
| Default severity | warning |
| Source stream | security |
| Message format string | Dynamic <i>\$vRtrIfDcpFpProtocol\$</i> policers freed for network_if <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> at <i>\$vRtrIfDcpTimeEventOccured\$</i> . Policy <i>\$vRtrIfDcpProtPolicy\$</i> . Excd count= <i>\$vRtrIfDcpFpDynExcdCount\$</i> |
| Cause | The vRtrIfDcpDynamicEnforceFreed notification is generated when a dynamic enforcement policer is freed on a particular network-interface. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtProtocolDynLogEvent is configured to 'verbose'. |
| Effect | The affected network-interface is now in conformance with the configured parameters of the associated distributed CPU protection policy. |
| Recovery | There is no recovery required for this notification. |

70.157 vRtrIfDcpDynamicExcd

Table 1468: 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 <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> detected at <i>\$vRtrIfDcpTimeEventOccured\$</i> . Policy <i>\$vRtrIfDcpProtPolicy\$</i> . Policer= <i>\$vRtrIfDcpFpProtocol\$(dynamic)</i> . Excd count= <i>\$vRtrIfDcpFpDynExcdCount\$</i> |

| Property name | Value |
|---------------|--|
| 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. |

70.158 vRtrIfDcpDynamicHoldDownEnd

Table 1469: 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 \$tmnxCardSlot Num\$/\$tmnxFPNum\$ at \$vRtrIfDcpTimeEventOccured\$. Policy \$vRtrIfDcpCpuProtPolicy\$. 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. |

70.159 vRtrIfDcpDynamicHoldDownStart

Table 1470: vRtrIfDcpDynamicHoldDownStart properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2069 |
| Event name | vRtrIfDcpDynamicHoldDownStart |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.50 |
| Default severity | warning |
| Source stream | security |
| Message format string | Hold-down started for network_if \$vRtrIfIndex\$ on fp \$tmnxCardSlotNum\$/\$tmnxFPNum\$ at \$vRtrIfDcpTimeEventOccured\$. Policy \$vRtrIfDcpCpuProtPolicy\$. 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. |

70.160 vRtrIfDcpLocMonExcd

Table 1471: vRtrIfDcpLocMonExcd properties

| Property name | Value |
|------------------|---------------------|
| Application name | SECURITY |
| Event ID | 2074 |
| Event name | vRtrIfDcpLocMonExcd |

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.55 |
| Default severity | warning |
| Source stream | security |
| Message format string | Local monitor <i>\$vRtrIfDcpFpLocMonPlcrName\$</i> for network_if <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> detected as non-conformant at <i>\$vRtrIfDcpTimeEventOccured\$</i> . Policy <i>\$vRtrIfDCpuProtPolicy\$</i> . Excd count= <i>\$vRtrIfDcpFpLocMonExcdCount\$</i> |
| Cause | The vRtrIfDcpLocMonExcd notification is generated when the local-monitoring-policer for a particular network-interface has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers. 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. 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. |

70.161 vRtrIfDcpLocMonExcdAllDynAlloc

Table 1472: 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 <i>\$vRtrIfDcpFpLocMonPlcrName\$</i> for network_if <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> at <i>\$vRtrIfDcpTimeEventOccured\$</i> . Policy <i>\$vRtrIfDCpuProtPolicy\$</i> . Excd count= <i>\$vRtrIfDcpFpLocMonExcdCount\$</i> |

| Property name | Value |
|---------------|---|
| 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. |

70.162 vRtrIfDcpLocMonExcdAllDynFreed

Table 1473: 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 \$vRtrIfDcpFpLocMonPlcrName\$ for network_if \$vRtrIfIndex\$ on fp \$tmnxCardSlotNum\$/\$tmnxFPNum\$ at \$vRtrIfDcpTimeEventOccured\$. Policy \$vRtrIfDcpProtPolicy\$. |
| 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. |

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

70.163 vRtrIfDcpLocMonExcdDynResource

Table 1474: vRtrIfDcpLocMonExcdDynResource properties

| Property name | Value |
|----------------------------------|--|
| Application name | SECURITY |
| Event ID | 2075 |
| Event name | vRtrIfDcpLocMonExcdDynResource |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.56 |
| Default severity | warning |
| Source stream | security |
| Message format string | Local monitor <i>\$vRtrIfDcpFpLocMonPlcrName\$</i> for network_if <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> detected as non-conformant at <i>\$vRtrIfDcpTimeEventOccured\$</i> and cannot allocate dynamic policers. Policy <i>\$vRtrIfDCpuProtPolicy\$</i> . Excd count= <i>\$vRtrIfDcpFpLocMonExcdCount\$</i> |
| 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). |

70.164 vRtrIfDcpStaticConform

Table 1475: vRtrIfDcpStaticConform properties

| Property name | Value |
|----------------------------------|---|
| Application name | SECURITY |
| Event ID | 2072 |
| Event name | vRtrIfDcpStaticConform |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.53 |
| Default severity | warning |
| Source stream | security |
| Message format string | Network_if \$vRtrIfIndex\$ on fp \$tmnxCardSlotNum\$/ \$tmnxFPNum \$ newly conformant at \$vRtrIfDcpTimeEventOccured\$. Policy \$vRtrIfDcpCpuProtPolicy\$. 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. |

70.165 vRtrIfDcpStaticExcd

Table 1476: vRtrIfDcpStaticExcd properties

| Property name | Value |
|------------------|----------|
| Application name | SECURITY |

| Property name | Value |
|----------------------------------|--|
| 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 \$vRtrIfDcpProtPolicy\$. Policer= \$vRtrIfDcpFpStaticPlcrName\$(static). Excd count=\$vRtrIfDcpFpStaticExcdCount\$ |
| Cause | The vRtrIfDcpStaticExcd notification is generated when the static-policer on a particular network-interface has been detected as non-conformant to the associated distributed CPU protection policy parameters. This notification is generated when TIMETRA-SECURITY-MIB.mib::tmnxDCpuProtStaticPlcrLogEvent is configured to 'enable' or 'verbose'. |
| Effect | The affected network-interface may be using more resources than expected and cause the system to under-perform. This notification may indicate a Denial of Service attack or a misconfiguration in the network. |
| Recovery | Appropriate configuration changes to the distributed CPU protection policy or to the affected network-interface may be required. |

70.166 vRtrIfDcpStaticHoldDownEnd

Table 1477: 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 |

| Property name | Value |
|-----------------------|--|
| Message format string | Hold-down completed for network_if <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> at <i>\$vRtrIfDcpTimeEventOccured\$</i> . Policy <i>\$vRtrIfDcpProtPolicy\$</i> . Policer= <i>\$vRtrIfDcpFpStaticPlcrName\$(static)</i> . Excd count= <i>\$vRtrIfDcpFpStaticExcdCount\$</i> |
| 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. |

70.167 vRtrIfDcpStaticHoldDownStart

Table 1478: 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 <i>\$vRtrIfIndex\$</i> on fp <i>\$tmnxCardSlotNum\$/\$tmnxFPNum\$</i> at <i>\$vRtrIfDcpTimeEventOccured\$</i> . Policy <i>\$vRtrIfDcpProtPolicy\$</i> . Policer= <i>\$vRtrIfDcpFpStaticPlcrName\$(static)</i> . Excd count= <i>\$vRtrIfDcpFpStaticExcdCount\$</i> |
| 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. |

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

71 SFLOW

71.1 tmnxSflowCpEntrySampling

Table 1479: 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 - <i>\$tmnxSflowNotifyFlowFailReason\$</i> |
| 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 1480: 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 - <i>\$tmnxSflowNotifyFlowFail Reason\$</i> |
| 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 1481: 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 <i>\$subject\$</i> , from IP <i>\$sourceUDP\$</i> |
| 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 1482: 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 1483: 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: <i>\$alarmDescription</i> |

| 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 1484: 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 <i>\$subject\$</i> 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 1485: 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 <i>\$subject\$</i> 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 1486: 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: <i>\$alarmDescription\$</i> |

| 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 1487: 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: <i>\$tmnxSnmpdErrorMsg\$</i> |
| Cause | The Snmp daemon detected an error. |
| Effect | N/A |
| Recovery | N/A |

72.8 warmStart

Table 1488: 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 1489: 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 <i>\$vRtrIfIndex\$</i> failure: <i>\$tmnxSrMplsNotifyDescription\$</i> |
| 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 1490: 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 <i>\$vRtrIfIndex\$</i> Flex Algo <i>\$tmnxSrMplsPfxSidFlexAlgoId\$</i> failure: <i>\$tmnxSrMplsNotifyDescription\$</i> |
| 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 1491: 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 <i>\$vRtrNotifSrv6ExhaustedRsrc\$</i> failed for router <i>\$vRtrID \$ \$vRtrNotifSrv6LocatorType\$ \$vRtrSrv6LocName\$</i> function <i>\$vRtrSrv6FunctionType\$</i> value <i>\$vRtrSrv6FunctionValue\$</i> . |
| 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 1492: 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 1493: 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 1494: 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 <i>\$tmnxCustomerBridgeId\$</i> with root bridge <i>\$tmnxCustomerRootBridgeId\$</i> has higher priority, for service <i>\$svclId\$</i> (customer <i>\$custId\$</i>) on SAP <i>\$sapEncapValue\$</i> |
| 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 1495: 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 <i>\$svcId\$</i> (customer <i>\$custId\$</i>) 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 1496: 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 <i>\$svcId\$</i> (customer <i>\$custId\$</i>) due to SAP <i>\$sapEncapValue\$</i> |
| 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 1497: 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) 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 1498: 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 <i>\$svclD\$</i> (customer <i>\$custld\$</i>) 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 1499: 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 <i>\$svclD\$</i> (customer <i>\$custld\$</i>) on SAP <i>\$sap EncapValue\$</i> |
| 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 1500: 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 <i>\$svcid\$</i> (customer <i>\$custId\$</i>) SAP <i>\$sapPortId\$:\$sapEncapValue\$</i> active protocol changed to <i>\$sapTlsStpOperProtocol\$</i> . |
| 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 1501: 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) SAP <i>\$sapEncapValue\$</i> encapsulation changed to 802.1d, bridged with <i>\$tmnxOtherBridgeId\$</i> |
| 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 1502: 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) SAP <i>\$sapEncapValue\$</i> encapsulation changed to PVST, bridged with <i>\$tmnxOtherBridgeId\$</i> |
| 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 1503: 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 <i>\$svcStpRegionalName\$</i> root <i>\$svcTlsStpCistRegionalRoot\$</i> elected in service <i>\$svclId\$</i> |
| 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 1504: 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 <i>\$tlMstiRegionalRoot\$</i> elected in service <i>\$svcId\$</i> . Msti-InstanceId: <i>\$svcMstiInstanceId\$</i> |
| 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 1505: 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) on PIP has changed to <i>\$tlSipStpException\$</i> |
| Cause | The STP exception state has changed. |
| Effect | N/A |
| Recovery | N/A |

75.13 tmnxSapStpExcepCondStateChng

Table 1506: 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) on SAP <i>\$sapEncapValue\$</i> has changed to <i>\$sapTlSipStpException\$</i> |

| Property name | Value |
|---------------|------------------------------------|
| Cause | A STP exception state has changed. |
| Effect | N/A |
| Recovery | N/A |

75.14 tmnxSdpBndStpExcepCondStateChng

Table 1507: 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 <i>\$sdpBindTlsStpException</i> \$ in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) on SDP Bind <i>\$sdpBindId\$</i> |
| Cause | The STP exception condition has changed on an SDP Binding." |
| Effect | N/A |
| Recovery | N/A |

75.15 tmnxStpMeshNotInMstRegion

Table 1508: 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 <i>\$sdpBindId\$</i> in service <i>\$svclD\$</i> . 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 1509: *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 <i>\$svclD\$</i> on SAP <i>\$sapEncapValue\$</i> |
| Cause | A STP detects a root-guard violation. |
| Effect | The query will be ignored. |
| Recovery | No recovery is necessary. |

75.17 tmnxSvcNewRootSdpBind

Table 1510: 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 <i>\$svcTlsStpDesignatedRoot\$</i> elected for service <i>\$svcl\$</i> (customer <i>\$custId\$</i>) due to SDP Bind <i>\$sdpBindId\$</i> |
| 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 1511: 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 <i>\$svcId\$</i> (customer <i>\$custId\$</i>) SDP Bind <i>\$sdpBindId\$</i> active changed to <i>\$sdpBindTIsStpOperProtocol\$</i> . |
| 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 1512: *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 <i>\$svcId\$</i> (customer <i>\$custId\$</i>) SDP Bind <i>\$sdpBindId\$</i> encapsulation changed to 802.1d, bridged with <i>\$tmnxOtherBridgeId\$</i> |
| 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 1513: *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 <i>\$svcId\$</i> (customer <i>\$custId\$</i>) SDP Bind <i>\$sdpBindId\$</i> encapsulation changed to PVST, bridged with <i>\$tmnxOtherBridgeId\$</i> |
| 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 1514: *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 <i>\$tmnxCustomerBridgeId\$</i> with root bridge <i>\$tmnxCustomerRootBridgeId\$</i> has higher priority, for service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) on SDP Bind <i>\$sdpBindId\$</i> |
| 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 1515: *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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) on SDP Bind <i>\$sdpBindId\$</i> |
| 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 1516: *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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) due to SDP Bind <i>\$sdpBindId\$</i> state change from <i>\$tmnxOldSdpBindTlsStpPortState\$</i> to <i>\$sdpBindTlsStpPortState\$</i> |
| 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 1517: 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>) due to SDP Bind <i>\$sdpBindId\$</i> state change from <i>\$tmnxOldSdpBindTlsStpPortState\$</i> to <i>\$sdpBindTlsStpPortState\$</i> |
| 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 1518: 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 <i>\$svcid\$</i> (customer <i>\$custId\$</i>) 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 1519: 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>) 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 1520: 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>) due to SAP <i>\$sapEncapValue\$</i> 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 1521: 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 <i>\$svcid\$</i> (customer <i>\$custId\$</i>) due to SAP <i>\$sapEncapValue\$</i> 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 1522: 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>) due to VCP state change to <i>\$tmnxVcpState\$</i> |
| 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 1523: 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>) to SDP <i>\$sdplD\$</i> 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 1524: 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 alulpTransportStateChanged

Table 1525: *alulpTransportStateChanged* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVCMGR |
| Event ID | 2573 |
| Event name | alulpTransportStateChanged |
| SNMP notification prefix and OID | ALU-IP-TRANSPORT-MIB.alulpTransportNotifications.1 |
| Default severity | minor |
| Source stream | main |
| Message format string | <i>IPT \$alulpTransportNotifyPortId\$ on service \$alulpTransportNotifySvcId\$ changed state to admin=\$alulpTransportAdminState\$ oper=\$alulpTransportOperState\$ flags= \$alulpTransportOperFlags\$</i> |
| 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 alulpTransportOperState indicates outOfService (or down), the IP Transport can no longer carry data over the network. |
| Recovery | The value of alulpTransportOperFlags will indicate what needs attention. |

76.2 dynamicSdpBindConfigChanged

Table 1526: *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 <i>\$dynamicSdpOrigin\$</i> SDP Bind <i>\$svcL2RteSdpBindId\$ \$sdpMSPwPeld\$</i> was <i>\$dynamicSdpStatus\$</i> . |
| 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 'sdpld' or by Spoke-SDP FEC identifier 'sdpMSPwPeld'. |
| 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 1527: *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 <i>\$dynamicSdpOrigin\$</i> SDP Bind on SDP <i>\$sdpId\$</i> for the following reason: <i>\$dynamicSdpBindCreationError\$</i> . |
| Cause | The system failed to create a dynamic SDP Bind. |
| Effect | N/A |
| Recovery | N/A |

76.4 dynamicSdpConfigChanged

Table 1528: *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 <i>\$dynamicSdpOrigin\$</i> SDP <i>\$sdpId\$</i> was <i>\$dynamicSdpStatus\$</i> . |
| Cause | A dynamic SDP was 'created', 'modified', or 'deleted'. |
| Effect | N/A |
| Recovery | N/A |

76.5 dynamicSdpCreationFailed

Table 1529: *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 <i>\$dynamicSdpOrigin\$</i> SDP for the following reason: <i>\$dynamicSdpCreationError\$</i> . |
| Cause | The system failed to create a dynamic SDP. |
| Effect | N/A |
| Recovery | N/A |

76.6 hostConnectivityLost

Table 1530: *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 <i>\$sapEncapValue\$</i> in service <i>\$svcid\$</i> for inet Addr = <i>\$hostConnectivityCiAddr\$</i> , chAddr= <i>\$hostConnectivityChAddr\$</i> , verify-addr= <i>\$sapNotifyIpAddr\$</i> . |
| Cause | The system lost the connectivity with a host. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

76.7 hostConnectivityRestored

Table 1531: hostConnectivityRestored properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> , for inetAddr = <i>\$hostConnectivityCiAddr\$</i> , chAddr= <i>\$hostConnectivityChAddr\$</i> , verify-addr= <i>\$sapNotifyIpAddr\$</i> . |
| Cause | Connectivity to a host has been restored. |
| Effect | N/A |
| Recovery | N/A |

76.8 iesIfStatusChanged

Table 1532: iesIfStatusChanged properties

| Property name | Value |
|----------------------------------|-----------------------------|
| Application name | SVC MGR |
| 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 <i>\$iesIfName\$</i> in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) changed to admin= <i>\$iesIfAdminStatus\$</i> oper= <i>\$iesIfOperStatus\$</i> |
| 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 1533: *msapCreationFailure* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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: <i>\$sapNotifyEncapValue\$</i> MAC: <i>\$sapTlsNotifyMacAddr\$</i> , Capturing SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svcId\$</i> . Description: <i>\$svcManagedSapCreationError\$</i> |
| Cause | The system failed to create a managed SAP. |
| Effect | N/A |
| Recovery | N/A |

76.10 msapStateChanged

Table 1534: *msapStateChanged* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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, <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> , has been <i>\$msapStatus\$</i> |
| Cause | A managed SAP was 'created', 'modified', or 'deleted'. |
| Effect | N/A |
| Recovery | N/A |

76.11 sapCemPacketDefectAlarm

Table 1535: *sapCemPacketDefectAlarm* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>): Alarm ' <i>\$sapCemReportAlarmStatus\$</i> ' 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 1536: sapCemPacketDefectAlarmClear properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> (customer <i>\$custId\$</i>): Alarm ' <i>\$sapCemReportAlarmStatus\$</i> ' 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 1537: sapEthLoopbackStarted properties

| Property name | Value |
|----------------------------------|-----------------------------|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$ \$sapEthLoopbackMode\$</i> in service <i>\$svcId\$</i> . |
| 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 1538: sapEthLoopbackStopped properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$ \$sapEthLoopbackMode\$</i> in service <i>\$svcId\$</i> . |
| 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 1539: sapHostBGPPeeringSetupFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$\$sapBGPPeeringHostIpAddr\$</i> on SAP: <i>\$\$sapEncapValue\$</i> , service: <i>\$\$svcId\$</i> . BGP peering attributes discarded: <i>\$\$sapBGPPeeringAttrDiscarded\$</i> . Description: <i>\$\$sapBGPPeeringNotifDescription\$</i> |
| 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 1540: sapHostRipListenerSetupFailed properties

| Property name | Value |
|----------------------------------|-------------------------------|
| Application name | SVC MGR |
| 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 <i>\$sapRipListenerHostIpAddr\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svcId\$</i> .Description: <i>\$sapRipListenerNotifDescription\$</i> |
| Cause | To be documented |
| Effect | To be documented |
| Recovery | No recovery is required on this system. |

76.17 saplflgnorePortStateStart

Table 1541: *saplflgnorePortStateStart* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2245 |
| Event name | saplflgnorePortStateStart |
| 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: <i>\$svcId\$</i> for IP interface <i>\$sapNotifyIfName\$</i> . |
| Cause | The saplflgnorePortStateStart 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 saplflgnorePortStateStop

Table 1542: sapIflgnorePortStateStop properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2246 |
| Event name | sapIflgnorePortStateStop |
| 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: \$svclD\$ for IP interface \$sapNotifyIfName\$. |
| Cause | The sapIflgnorePortStateStop 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 sapIpipeCelpAddrChange

Table 1543: sapIpipeCelpAddrChange properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2543 |
| Event name | sapIpipeCelpAddrChange |
| SNMP notification prefix and OID | TIMETRA-SAP-MIB.sapTraps.33 |
| Default severity | minor |
| Source stream | main |
| Message format string | CE IP address \$sapIpipeCelpAddress\$ is discovered on Ipipe SAP \$sapEncapValue\$ in service \$svclD\$. |
| Cause | The sapIpipeCelpAddrChange 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 sapIpPipeCelpAddrType. The IP address is specified by sapIpPipeCelpAddress. |
| Effect | The IP address specified by sapIpPipeCelpAddress and of type sapIpPipeCelpAddrType has been discovered for the local end host. |
| Recovery | No action is required. |

76.20 sapPortStateChangeProcessed

Table 1544: sapPortStateChangeProcessed properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sapNotifyPortId\$</i> 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 sapPortStateChangeProcessed event is generated. |
| Recovery | N/A |

76.21 sapReceivedPbbProtSrcMac

Table 1545: 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 <i>\$protectedMacForNotify\$</i> protected in i-vpls <i>\$svclId\$</i> received on SAP <i>\$sapEncapValue\$</i> in b-vpls service <i>\$svcTlsBackboneVplsSvclId\$</i> . |
| Cause | The sapReceivedPbbProtSrcMac notification is generated when a protected source MAC protected in i-vpls is received on SAP in b-vpls (svcTlsBackboneVplsSvclId) service. |
| Effect | The frame is discarded. |
| Recovery | None needed. |

76.22 sapReceivedProtSrcMac

Table 1546: 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 <i>\$protectedMacForNotify\$</i> received on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> . |
| Cause | A protected source MAC was received on a TLS SAP. |

| Property name | Value |
|---------------|-------|
| Effect | N/A |
| Recovery | N/A |

76.23 sapStatusChanged

Table 1547: sapStatusChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> (customer <i>\$custId\$</i>) changed to admin= <i>\$sapAdminStatus\$</i> oper= <i>\$sapOperStatus\$</i> flags= <i>\$sapOperFlags\$</i> |
| 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 1548: sapTlsDataSapInstStatusChgd properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |

| 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 <i>\$svcId\$</i> SAP <i>\$sapEncapValue\$</i> changed to <i>\$sapTlsDataSapInstStatus\$</i> with last-error: <i>\$sapTlsDataSapInstLastErr\$</i> |
| Cause | Data SAP instantiation status changed |
| Effect | N/A |
| Recovery | N/A |

76.25 sapTlsMacAddrLimitAlarmCleared

Table 1549: sapTlsMacAddrLimitAlarmCleared properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> 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 sapTIsMacAddrLimitAlarmRaised

Table 1550: sapTIsMacAddrLimitAlarmRaised properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVCMGR |
| Event ID | 2204 |
| Event name | sapTIsMacAddrLimitAlarmRaised |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> 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 sapTIsMacMoveExceeded

Table 1551: sapTIsMacMoveExceeded properties

| Property name | Value |
|----------------------------------|-----------------------------|
| Application name | SVCMGR |
| Event ID | 2209 |
| Event name | sapTIsMacMoveExceeded |
| 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>), MAC <i>\$sapTlsNotifyMacAddr\$</i> exceeded <i>\$svcTlsMacMoveMaxRate\$</i> and will retry in <i>\$sapTlsMacMoveNextUpTime\$</i> seconds (retries left= <i>\$sapTlsMacMoveRateExcdLeft\$</i> admin= <i>\$sapAdminStatus\$</i> oper= <i>\$sapOperStatus\$</i>) - detected on SAP <i>\$sapEncapValue\$</i> |
| Cause | The TLS <i>svcTlsMacMoveMaxRate</i> has been exceeded for the SAP. |
| Effect | The interface will be brought down and then brought back up automatically in <i>sapTlsMacMoveNextUpTime</i> seconds if retries are left as indicated by <i>sapTlsMacMoveRateExcdLeft</i> . |
| Recovery | If there are retries left, as indicated by <i>sapTlsMacMoveRateExcdLeft</i> , the interface will be brought back up automatically in <i>sapTlsMacMoveNextUpTime</i> seconds. If no retries are left, the interface must be manually brought back up by an administrator. |

76.28 sapTlsMacMoveExceedNonBlock

Table 1552: sapTlsMacMoveExceedNonBlock properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>), MAC <i>\$sapTlsNotifyMacAddr\$</i> exceeded <i>\$svcTlsMacMoveMaxRate\$</i> - detected on SAP <i>\$sapEncapValue\$</i> |
| Cause | The <i>sapTlsMacMoveExceedNonBlock</i> notification is generated when the SAP exceeds the TLS <i>svcTlsMacMoveMaxRate</i> when <i>sapTlsLimitMacMove</i> 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 <i>svclD</i> , <i>custId</i> of I-VPLS and B-VPLS <i>sapId</i> . |

| 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 1553: sapTunnelEncapIpMtuTooSmall properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$sapTunnelNotifyName</i> on SAP: <i>\$sapEncapValue</i> , service: <i>\$svclId</i> with configured MTU of <i>\$sapTunnelNotifyConfigIpMtu</i> , having encapsulated MTU of <i>\$sapTunnelNotifyConfigEncapIpMtu</i> has an overhead of <i>\$sapTunnelNotifyEncapOverhead</i> . |
| 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 1554: sapTunnelStateChange properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$sapTunnelNotifyName\$</i> has changed to <i>\$sapTunnelNotifyState\$</i> due to <i>\$sapTunnelNotifyReason\$</i> |
| Cause | The trap sapTunnelStateChange is sent when IPsec/GRE tunnel indicated by sapTunnelNotifyName changes state to 'down' due to sapTunnelNotifyReason. |
| 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 1555: sdpBandwidthOverbooked properties

| Property name | Value |
|----------------------------------|-----------------------------|
| Application name | SVC MGR |
| 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 <i>\$sdpBookedBandwidth\$</i> of SDP <i>\$sdpId\$</i> has exceeded the max bookable bandwidth <i>\$sdpMaxBookableBandwidth\$</i> . |
| 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 1556: 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 <i>\$sdpBindId\$</i> <i>\$sdpBindEthLoopbackMode\$</i> in service <i>\$svclId\$</i> . |
| 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 1557: *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 <i>\$sdpBindId\$ \$sdpBindEthLoopback Mode\$</i> in service <i>\$svcId\$</i> . |
| 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 1558: *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 <i>\$sdpAvailableBandwidth\$</i> of SDP cannot satisfy the bandwidth <i>\$sdpBindAdminBandwidth\$</i> required by the SDP Bind <i>\$sdpBindId\$</i> . |

| 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 sdpBindIpipeCelpAddressChange

Table 1559: sdpBindIpipeCelpAddressChange properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2324 |
| Event name | sdpBindIpipeCelpAddressChange |
| SNMP notification prefix and OID | TIMETRA-SDP-MIB.sdpTraps.29 |
| Default severity | minor |
| Source stream | main |
| Message format string | CE IP address <i>\$sdpBindIpipeCelpAddress\$</i> is discovered on Ipipe SDP bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> . |
| Cause | The sdpBindIpipeCelpAddressChange 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 sdpBindIpipeCelpAddrType. The IP address is specified by sdpBindIpipeCelpAddress. |
| Effect | The IP address specified by sdpBindIpipeCelpAddress and of type sdpBindIpipeCelpAddrType has been discovered on the remote CE device. |
| Recovery | No action is required. |

76.36 sdpBindPwLocalStatusBitsChanged

Table 1560: *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 <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) local PW status bits changed to <i>\$sdpBindPwLocalStatusBitsString\$</i> |
| 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 1561: *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 <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) peer PW status IP address changed to <i>\$sdpBindPwFaultInetAddress\$</i> |

| 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 1562: sdpBindPwPeerStatusBitsChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) peer PW status bits changed to <i>\$sdpBindPwPeerStatusBitsString\$</i> |
| Cause | There was a change in the PW status bits received from the peer. |
| Effect | N/A |
| Recovery | N/A |

76.39 sdpBindReceivedPbbProtSrcMac

Table 1563: *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 <i>\$protectedMacForNotify\$</i> protected in i-vpls <i>\$svclD\$</i> is received on SDP Bind <i>\$sdpBindId\$</i> in b-vpls service <i>\$svcTIsBackboneVplsSvclD\$</i> . |
| 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 (svcTIsBackboneVplsSvclD) service. |
| Effect | The frame will be discarded. |
| Recovery | No action is required. |

76.40 sdpBindReceivedProtSrcMac

Table 1564: *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 <i>\$protectedMacForNotify\$</i> received on SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclD\$</i> . |

| 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 1565: 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 <i>\$sdpNotifySdpId\$</i> 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 1566: *sdpBindStatusChanged* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) changed to admin= <i>\$sdpBindAdminStatus\$</i> oper= <i>\$sdpBindOperStatus\$</i> flags= <i>\$sdpBindOperFlags\$</i> |
| 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 sdpBindTIsMacMoveExceeded

Table 1567: *sdpBindTIsMacMoveExceeded* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2314 |
| Event name | sdpBindTIsMacMoveExceeded |
| SNMP notification prefix and OID | TIMETRA-SDP-MIB.sdpTraps.15 |
| Default severity | minor |
| Source stream | main |
| Message format string | Mac move rate for service <i>\$svcId\$</i> (customer <i>\$custId\$</i>), MAC <i>\$sdpBindNotifyMacAddr\$</i> exceeded <i>\$svcTIsMacMoveMaxRate\$</i> and will retry in <i>\$sdpBindTIsMacMoveNextUpTime\$</i> seconds (retries left= <i>\$sdpBindTIs</i> |

| Property name | Value |
|---------------|---|
| | <i>MacMoveRateExcdLeft\$ admin= \$sdpBindAdminStatus\$ oper=\$sdpBindOperStatus\$) - detected on SDP Bind \$sdpBindId\$</i> |
| Cause | This notification is generated when the TLS svcTlsMacMoveMaxRate has been exceeded for the SDP Bind. |
| Effect | The interface will be brought down and then brought back up automatically in sdpBindTlsMacMoveNextUpTime seconds if retries are remaining as indicated by sdpBindTlsMacMoveRateExcdLeft. |
| Recovery | If there are retries remaining, as indicated by sdpBindTlsMacMoveRateExcdLeft, the interface will be brought back up automatically in sdpBindTlsMacMoveNextUpTime seconds. If no retries are remaining, the interface must be manually brought back up by an administrator. |

76.44 sdpBindTlsMacMoveExceedNonBlock

Table 1568: sdpBindTlsMacMoveExceedNonBlock properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$svclId\$</i> (customer <i>\$custId\$</i>), MAC <i>\$sdpBindNotifyMacAddr\$</i> exceeded <i>\$svcTlsMacMoveMaxRate\$</i> - detected on SDP Bind <i>\$sdpBindId\$</i> |
| 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 svclId, 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 1569: sdpControlPwActiveStateChg properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$sdpControlPWIsActive\$</i> on SDP: <i>\$sdpId\$</i> |
| 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 sdpEgrlfsNetDomInconsCntChanged

Table 1570: sdpEgrlfsNetDomInconsCntChanged properties

| Property name | Value |
|----------------------------------|---------------------------------|
| Application name | SVC MGR |
| Event ID | 2323 |
| Event name | sdpEgrlfsNetDomInconsCntChanged |
| 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 <i>\$sdpEglfNetDomainInconsCount\$</i> 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 1571: *sdpKeepAliveLateReply* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2310 |
| Event name | sdpKeepAliveLateReply |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | main |
| Message format string | SDP <i>\$sdpId\$</i> probe <i>\$probeSeqNumber\$</i> response comes after timeout |
| Cause | A SDP keep alive session received a late reply. |
| Effect | N/A |
| Recovery | N/A |

76.48 sdpKeepAliveProbeFailure

Table 1572: *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 <i>\$sdpId\$</i> : failed with error: <i>\$Error\$</i> |
| Cause | A sdp keep alive probe has not responded correctly. |
| Effect | N/A |
| Recovery | N/A |

76.49 sdpKeepAliveStarted

Table 1573: *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 <i>\$sdpId\$</i> keepalive has started |
| Cause | A sdp keep alive was started. |
| Effect | N/A |
| Recovery | N/A |

76.50 sdpKeepAliveStopped

Table 1574: sdpKeepAliveStopped properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2308 |
| Event name | sdpKeepAliveStopped |
| SNMP notification prefix and OID | N/A |
| Default severity | minor |
| Source stream | main |
| Message format string | SDP <i>\$sdpld\$</i> keepalive has stopped |
| Cause | A sdp keep alive was stopped. |
| Effect | N/A |
| Recovery | N/A |

76.51 sdpPbbActvPwWithNonActvCtrlPwChg

Table 1575: sdpPbbActvPwWithNonActvCtrlPwChg properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 (<i>\$sdpPbbActvPwWithNonActvCtrlPw\$</i>) on the BEB where control PW is standby/down on SDP: <i>\$sdpld\$</i> |

| 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 sdpPbbActvPwWithNonActvCtrlPw set to 'false' indicate clearing of sdpPbbActvPwWithNonActvCtrlPwChg with sdpPbbActvPwWithNonActvCtrlPw set to 'true'." |

76.52 sdpStatusChanged

Table 1576: sdpStatusChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sdpId\$</i> changed to admin= <i>\$sdpAdminStatus\$</i> oper= <i>\$sdpOperStatus\$</i> |
| Cause | There was a change in the administrative or operating status of an SDP. |
| Effect | N/A |
| Recovery | N/A |

76.53 sdpTlsMacAddrLimitAlarmCleared

Table 1577: *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 <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> 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 1578: *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 <i>\$sdpBindId\$</i> in service <i>\$svcId\$</i> 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 1579: svcArpHostOverride properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 1580: svcArpHostPopulateErr properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> - <i>\$svcArpHostPopulateError\$</i> |
| 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 <i>svcArpHostPopulateError</i> . |
| 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 1581: *svcBgpEvpnBHDupMacAddrsDetected* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVCNMR |
| 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 <i>\$svcId\$</i> failed to install black hole destination in FDB for EVPN detected duplicate MAC <i>\$tlfFdbMacAddr\$</i> . |
| Cause | The <i>svcBgpEvpnBHDupMacAddrsDetected</i> 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 1582: svcBgpEvpnDupMacAddrsCleared properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 \$svclId 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 1583: svcBgpEvpnDupMacAddrsDetected properties

| Property name | Value |
|----------------------------------|-------------------------------|
| Application name | SVC MGR |
| 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 \$svclId\$ 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 1584: svcBgpEvpnTepStateChgd properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 \$svclId\$ 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 1585: *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 1586: *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 1587: svcEndPointMacLimitAlarmCleared properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 1588: *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 1589: *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 1590: svcEPMCEPConfigMismatch properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$svcEndPointMCEPId\$</i> associated with endpoint " <i>\$svcEndPointName\$</i> " in service <i>\$svcId\$</i> 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 1591: svcEPMCEPConfigMismatchResolved properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |

| 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 <i>\$svcEndPointMCEPId\$</i> associated with endpoint " <i>\$svcEndPointName\$</i> " in service <i>\$svcId\$</i> 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 1592: *svcEPMCEPPassiveModeActive* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$svcEndPointMCEPId\$</i> associated with endpoint " <i>\$svcEndPointName\$</i> " in service <i>\$svcId\$</i> 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 1593: 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 <i>\$svcEndPointMCEPID\$</i> associated with endpoint " <i>\$svcEndPointName\$</i> " in service <i>\$svcid\$</i> 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 1594: 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 <i>\$svcNotifEthSeg Name\$</i> |
| 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 1595: svcEvpnESVxVTepLclBiasAddFailSet properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$svcNotifEthSeg Name\$</i> |
| 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 svcNotiflNetAddr. |
| 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 1596: 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 1597: 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 1598: svcEvpnMHAutoEsiConflict properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxSvcSysEthSegName\$</i> because the new ID <i>\$tmnxSvcSysEthSegEsi\$</i> conflicts with ES <i>\$tmnxSvcSysConflictingEthSegName\$</i> |
| 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 1599: svcEvpnMHAutoEsiCreated properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$tmnxSvcSysEthSegEsi\$</i> has been automatically created for Ethernet Segment <i>\$tmnxSvcSysEthSegName\$</i> |
| 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 1600: svcEvpnMHESeviDFStateChgd properties

| Property name | Value |
|------------------|---------------------------|
| Application name | SVC MGR |
| 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: <i>\$tmnxSvcSysEthSegName\$</i> , EVI: <i>\$svcEvpnMHEthSegEvi\$</i> , Designated Forwarding state changed to: <i>\$svcEvpnMHEthSegEvilsDF\$</i> |
| 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 1601: svcEvpnMHEsIsidDFStateChgd properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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: <i>\$tmnxSvcSysEthSegName\$</i> , ISID: <i>\$svcEvpnMHEthSegIsid\$</i> , Designated Forwarding state changed to: <i>\$svcEvpnMHEthSegIsidsDF\$</i> |
| 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 svcEvpnMplsESDestTEPStateChgd

Table 1602: svcEvpnMplsESDestTEPStateChgd properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2133 |
| Event name | svcEvpnMplsESDestTEPStateChgd |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.118 |
| Default severity | minor |
| Source stream | main |
| 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. |

76.79 svcEvpnMplsMacMoveExceedNonBlock

Table 1603: svcEvpnMplsMacMoveExceedNonBlock properties

| Property name | Value |
|----------------------------------|----------------------------------|
| Application name | SVC MGR |
| Event ID | 2068 |
| Event name | svcEvpnMplsMacMoveExceedNonBlock |
| SNMP notification prefix and OID | TIMETRA-SAP-MIB.sapTraps.60 |

| Property name | Value |
|-----------------------|--|
| Default severity | minor |
| Source stream | main |
| Message format string | Mac move rate for service <i>\$svclId\$</i> (customer <i>\$custId\$</i>), MAC <i>\$sapTlsNotifyMacAddr\$</i> exceeded <i>\$svcTlsMacMoveMaxRate\$</i> - detected on <i>\$tlsFdbBackboneDstMac\$</i> |
| Cause | The svcEvpnMplsMacMoveExceedNonBlock notification is generated when the EVPN MPLS destination exceeds the TLS svcTlsMacMoveMaxRate when sapTlsLimitMacMove is set to 'nonBlocking'. |
| Effect | This notification is informational only. |
| Recovery | User can adjust the value of svcTlsMacMoveMaxRate to reduce the frequency of this notification. |

76.80 svcEvpnMplsMldpESLbIHUsgClr

Table 1604: svcEvpnMplsMldpESLbIHUsgClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2621 |
| Event name | svcEvpnMplsMldpESLbIHUsgClr |
| 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 svcEvpnMplsMldpESLbIHUsgClr 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. |

76.81 svcEvpnMplsMldpESLbHiUsgSet

Table 1605: svcEvpnMplsMldpESLbHiUsgSet properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2620 |
| Event name | svcEvpnMplsMldpESLbHiUsgSet |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.121 |
| Default severity | minor |
| Source stream | main |
| Message format string | The number of MLDP EVPN ES labels programmed exceeds 95% of the system limit |
| Cause | The svcEvpnMplsMldpESLbHiUsgSet 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. |

76.82 svcEvpnMplsTEPEgrBndSvcHiUsgClr

Table 1606: svcEvpnMplsTEPEgrBndSvcHiUsgClr properties

| Property name | Value |
|----------------------------------|---------------------------------|
| Application name | SVC MGR |
| Event ID | 2357 |
| Event name | svcEvpnMplsTEPEgrBndSvcHiUsgClr |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.67 |
| Default severity | minor |

| Property name | Value |
|-----------------------|--|
| Source stream | main |
| Message format string | Service <i>\$svcId\$</i> has EVPN MPLS tunnel endpoint-egress multicast binds below 90% of the per-service limit |
| Cause | The <i>svcEvpnMplsTEPEgrBndSvcHiUsgClr</i> 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. |

76.83 svcEvpnMplsTEPEgrBndSvcHiUsgSet

Table 1607: *svcEvpnMplsTEPEgrBndSvcHiUsgSet* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2356 |
| Event name | <i>svcEvpnMplsTEPEgrBndSvcHiUsgSet</i> |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB. <i>svcTraps.66</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Service <i>\$svcId\$</i> has EVPN MPLS tunnel endpoint-egress multicast binds in excess of 95% of the per-service limit |
| Cause | The <i>svcEvpnMplsTEPEgrBndSvcHiUsgSet</i> 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. |

76.84 svcEvpnMplsTEPEgrBndSysHiUsgClr

Table 1608: svcEvpnMplsTEPEgrBndSysHiUsgClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2355 |
| Event name | svcEvpnMplsTEPEgrBndSysHiUsgClr |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.65 |
| Default severity | minor |
| 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. |

76.85 svcEvpnMplsTEPEgrBndSysHiUsgSet

Table 1609: svcEvpnMplsTEPEgrBndSysHiUsgSet properties

| Property name | Value |
|----------------------------------|---------------------------------|
| Application name | SVC MGR |
| Event ID | 2354 |
| Event name | svcEvpnMplsTEPEgrBndSysHiUsgSet |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.64 |
| Default severity | minor |

| Property name | Value |
|-----------------------|--|
| 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. |

76.86 svcEvpnMplsTEPEgrLblStateChgd

Table 1610: svcEvpnMplsTEPEgrLblStateChgd properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 \$svclD\$ bgp-instance \$svcBgpEvpnInstance\$ with label \$svcEvpnMplsTEPEgrLblTEPLabel\$ in tunnel \$svcEvpnInstMplsTEPEgrLblTEPTnId\$ 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. |

76.87 svcEvpnMplsTEPHiUsageCleared

Table 1611: svcEvpnMplsTEPHiUsageCleared properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVCMGR |
| Event ID | 2353 |
| Event name | svcEvpnMplsTEPHiUsageCleared |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.63 |
| Default severity | minor |
| 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. |

76.88 svcEvpnMplsTEPHiUsageRaised

Table 1612: 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 |

| Property name | Value |
|-----------------------|--|
| 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. |

76.89 svcEvpnMplsTEPIpSysHiUsgClr

Table 1613: svcEvpnMplsTEPIpSysHiUsgClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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. |

76.90 svcEvpnMplsTEPIpSysHiUsgSet

Table 1614: *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 |
| 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. |

76.91 svcEvpnRcvdPbbProtSrcMac

Table 1615: *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 <i>\$protectedMacForNotify\$</i> protected in i-vpls <i>\$svcid\$</i> received on EVPN in b-vpls service <i>\$svcTlsBackboneVplsSvclid\$</i> . |

| Property name | Value |
|---------------|---|
| 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. |

76.92 svcEvpnRcvdProtSrcMac

Table 1616: svcEvpnRcvdProtSrcMac properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$protectedMacForNotify\$</i> received over EVPN in service <i>\$svcId\$</i> . |
| Cause | The svcEvpnRcvdProtSrcMac notification is generated when a protected source MAC is received. |
| Effect | The frame is discarded. |
| Recovery | None needed. |

76.93 svcEvpnVxInstESDstTEPStateChgd

Table 1617: svcEvpnVxInstESDstTEPStateChgd properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |

| Property name | Value |
|----------------------------------|--|
| 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 <i>\$svcEvpnVxlanInstESDstTEPAddress\$</i> in service <i>\$svcl\$</i> <i>\$ vxlan-instance \$svcVxlanInstanceId\$</i> with vni <i>\$svcEvpnVxlanInstESDstTEPVni\$</i> on <i>\$tmnxSvcSysEthSegEsi\$</i> has changed operational status to (<i>\$svcEvpnVxlanInstESDestTEPOpState\$</i>) and oper-flags (<i>\$svcEvpnVxlanInstESDestTEPOpFlag\$</i>) |
| 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. |

76.94 svcEvpnVxInstMHStandbyStatusChg

Table 1618: svcEvpnVxInstMHStandbyStatusChg properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2629 |
| Event name | svcEvpnVxInstMHStandbyStatusChg |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.127 |
| Default severity | minor |
| Source stream | main |
| Message format string | Vxlan Instance <i>\$svcNotifVxlanInstance\$</i> on service <i>\$svcl\$</i> multi-homing standby <i>\$svcNotifEvpnMHStandbyStatus\$</i> |
| Cause | The svcEvpnVxInstMHStandbyStatusChg notification is generated when there is a change in status of EVPN VXLAN instance multi-homing standby. |

| Property name | Value |
|---------------|--|
| Effect | EVPN VXLAN instance multi-homing standby status has changed. |
| Recovery | None needed. |

76.95 svcEvpnVxVTepLclBiasAddFailClr

Table 1619: svcEvpnVxVTepLclBiasAddFailClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 \$svcNotiflnetAddr\$ |
| Cause | The trap svcEvpnVxVTepLclBiasAddFailClr is sent whenever local bias failure condition for the Vxlan VTEP svcNotiflnetAddr, is cleared. |
| Effect | Vxlan local bias is enabled for the VTEP. |
| Recovery | None needed."; |

76.96 svcEvpnVxVTepLclBiasAddFailSet

Table 1620: svcEvpnVxVTepLclBiasAddFailSet properties

| Property name | Value |
|------------------|--------------------------------|
| Application name | SVC MGR |
| Event ID | 2114 |
| Event name | svcEvpnVxVTepLclBiasAddFailSet |

| Property name | Value |
|----------------------------------|---|
| 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 <i>\$svcNotiflNetAddr\$</i> due to system limit |
| Cause | The trap <i>svcEvpnVxVTepLclBiasAddFailSet</i> is sent whenever local bias cannot be enabled for the Vxlan VTEP <i>svcNotiflNetAddr</i> , 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 1621: *svcFdbMimDestTblFullAlrm* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2515 |
| Event name | <i>svcFdbMimDestTblFullAlrm</i> |
| 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 <i>\$svcTotalFdbMimDestIdxEntries\$</i> 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 <i>svcTotalFdbMimDestIdxEntries</i> object remains under 10 percent of the limit. |
| Recovery | N/A |

76.98 svcFdbMimDestTblFullAlarmCleared

Table 1622: svcFdbMimDestTblFullAlarmCleared properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2516 |
| Event name | svcFdbMimDestTblFullAlarmCleared |
| 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 <i>\$svcTotalFdbMimDestIdxEntries\$</i> 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 svclFSubForwardingStatsDisNotify

Table 1623: svclFSubForwardingStatsDisNotify properties

| Property name | Value |
|----------------------------------|----------------------------------|
| Application name | SVC MGR |
| Event ID | 2614 |
| Event name | svclFSubForwardingStatsDisNotify |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.108 |
| Default severity | minor |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | Statistics for subscriber/group-interface %iesIfIndex% disabled: %tmnx FailureDescription% |
| Cause | The svclFSubForwardingStatsDisNotify 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 svclFSubForwardingStatsEnNotify

Table 1624: svclFSubForwardingStatsEnNotify properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2615 |
| Event name | svclFSubForwardingStatsEnNotify |
| 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 svclFSubForwardingStatsEnNotify notification is generated when previously disabled subscriber/group-interface statistics are enabled again due to available resources. |
| Effect | A log entry is generated. |
| Recovery | None. |

76.101 svcMSPwRetryExpiredNotif

Table 1625: 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: \$svcMSPwPeld\$ in service: \$svclD\$ |
| Cause | The svcMSPwRetryExpiredNotif notification is raised when retry-timer expires for this multi-segment pseudo-wire provider-edge (svcMSPwPeld) in the service. |
| Effect | There will be no more retries to establish connection from this svcMSPwPeld. |
| Recovery | svcMSPwPeld may need to be shutdown and may need to restart the retries." |

76.102 svcMSPwRtMisconfig

Table 1626: 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 |
| Source stream | main |
| Message format string | Misconfigured multi-segment pseudo-wire SAll=\$svcMSPwPeSaiiGlobalId\$: \$svcMSPwPeSaiiPrefix\$: \$svcMSPwPeSaiiAcId\$ TAIL= |

| Property name | Value |
|---------------|---|
| | <i>\$svcMSPwPeTiiGlobalId\$:\$svcMSPwPeTiiPrefix\$:\$svcMSPwPeTiiAcld\$</i> |
| 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 1627: 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 <i>\$svcOperGrpName\$</i> changed status to <i>\$svcOperGrpOperStatus\$</i> |
| 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 1628: *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 1629: *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\$ |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

76.106 svcRoutedVplsEvpnGWDrStateChgd

Table 1630: svcRoutedVplsEvpnGWDrStateChgd properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 \$svclId\$ |
| 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 1631: svcRvplsEvpnMcastDestSysHiUsgClr properties

| Property name | Value |
|----------------------------------|----------------------------------|
| Application name | SVC MGR |
| Event ID | 2626 |
| Event name | svcRvplsEvpnMcastDestSysHiUsgClr |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.126 |

| Property name | Value |
|-----------------------|---|
| 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 1632: svcRvplsEvpnMcastDestSysHiUsgSet properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 |
| 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 1633: *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: <i>\$svcId\$</i> site: <i>\$svcNotifSiteName\$</i> min-down-timer state changed to: <i>\$svcNotifSiteMinDnTimerState\$</i> with timer: <i>\$svcNotifSiteMinDnTimer\$</i> secs and timer-remaining: <i>\$svcNotifSiteMinDnTimerRemain\$</i> secs |
| Cause | The <i>svcSiteMinDnTimerStateChg</i> notification is generated when site specific minimum-down-timer starts/canceled/extended/expires. |
| Effect | <i>svcSiteMinDnTimerState</i> indicate the new state of the site minimum-down-timer. |
| Recovery | None needed. |

76.110 *svcSrv6FunctionOutOfResources*

Table 1634: *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 <i>\$svcNotifSrv6ExhaustedResource\$</i> failed for <i>\$svcType\$</i> <i>\$svcId\$</i> srv6-instance <i>\$svcNotifSrv6Instance\$</i> <i>\$svcNotifSrv6Locator</i> |

| Property name | Value |
|---------------|--|
| | 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 1635: 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 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 1636: 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 (\$svcSrv6InstTEPSidOperFlag\$) |
| 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 1637: 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 |

| Property name | Value |
|---------------|--|
| 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 1638: svcSrv6TEPEgrBndSvcHiUsgSet properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 |
| 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 1639: svcSrv6TEPEgrBndSysHiUsgClr properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 1640: svcSrv6TEPEgrBndSysHiUsgSet properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 |

| Property name | Value |
|---------------|--|
| 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 1641: svcStatusChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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: \$svcOperStatus\$ |
| Cause | There was a change in the administrative or operating status of a service. |
| Effect | N/A |
| Recovery | N/A |

76.118 svcSysEvpnESDfPrefOperValChange

Table 1642: 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: <i>\$tmnxSvcSysEthSegName\$</i> , The Oper DF preference value changed to <i>\$svcSysEvpnESDfPrefElecOperValue\$</i> and/or the DP value changed to <i>\$svcSysEvpnESDfPrefElecDntPreempt\$</i> . |
| 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 1643: 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 <i>\$svclid\$</i> |

| Property name | Value |
|---------------|--|
| 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 1644: svcTlsEvpnTunnNHopHiUsgAlarmSet properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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\$ |
| 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 1645: svcTIsFdbTableFullAlarmCleared properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVCMGR |
| Event ID | 2105 |
| Event name | svcTIsFdbTableFullAlarmCleared |
| 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 svcTIsFdbTableFullAlarmRaised

Table 1646: svcTIsFdbTableFullAlarmRaised properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVCMGR |
| Event ID | 2104 |
| Event name | svcTIsFdbTableFullAlarmRaised |
| 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 |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

76.123 svcTlsGroupOperStatusChanged

Table 1647: 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 \$svcTlsGroupOperStatus\$ with last-error: \$svcTlsGroupLastError\$ |
| Cause | Service VPLS Group status changed |
| Effect | N/A |
| Recovery | N/A |

76.124 svcTlsMacPinningViolation

Table 1648: svcTlsMacPinningViolation properties

| Property name | Value |
|----------------------------------|------------------------------|
| Application name | SVCMGR |
| Event ID | 2011 |
| Event name | svcTlsMacPinningViolation |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.11 |

| Property name | Value |
|-----------------------|--|
| Default severity | warning |
| Source stream | main |
| Message format string | Relearn attempt on <i>\$macPinningViolatingRowDescr\$</i> in service <i>\$svclId\$</i> for mac address <i>\$macPinningMacAddress\$</i> pinned on <i>\$macPinningPinnedRowDescr\$</i> |
| 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 svcTIsMfibTableFullAlarmCleared

Table 1649: *svcTIsMfibTableFullAlarmCleared* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2402 |
| Event name | svcTIsMfibTableFullAlarmCleared |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.10 |
| Default severity | minor |
| Source stream | main |
| Message format string | MFIB table utilization of service <i>\$svclId\$</i> (customer <i>\$custId\$</i>) 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 svcTIsMfibTableFullAlarmRaised

Table 1650: svcTIsMfibTableFullAlarmRaised properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2401 |
| Event name | svcTIsMfibTableFullAlarmRaised |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.9 |
| Default severity | minor |
| Source stream | main |
| Message format string | MFIB table utilization of service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) crossed its high watermark |
| Cause | The utilization of the MFIB table rose above the high watermark. |
| Effect | N/A |
| Recovery | N/A |

76.127 svcTIsMrpAttrRegistrationFailed

Table 1651: svcTIsMrpAttrRegistrationFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2120 |
| Event name | svcTIsMrpAttrRegistrationFailed |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.20 |
| Default severity | minor |
| Source stream | main |
| Message format string | An MRP attribute with type= <i>\$svcTIsMrpAttrType\$</i> value= <i>\$svcTIsMrpAttrValue</i> failed to register in service <i>\$svcId\$</i> (customer <i>\$custId\$</i>) due to: <i>\$svcTIsMrpAttrRegFailedReason\$</i> |
| Cause | An MRP attributed failed to register in a service. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

76.128 svcTlsMrpAttrTbIFullAlarmCleared

Table 1652: svcTlsMrpAttrTbIFullAlarmCleared properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVCMGR |
| Event ID | 2126 |
| Event name | svcTlsMrpAttrTbIFullAlarmCleared |
| 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 <i>\$svcId\$</i> (customer <i>\$custId\$</i>) crossed its low watermark |
| Cause | The utilization of the MRP attribute table fell below the low watermark. |
| Effect | N/A |
| Recovery | N/A |

76.129 svcTlsMrpAttrTbIFullAlarmRaised

Table 1653: svcTlsMrpAttrTbIFullAlarmRaised properties

| Property name | Value |
|----------------------------------|---------------------------------|
| Application name | SVCMGR |
| Event ID | 2125 |
| Event name | svcTlsMrpAttrTbIFullAlarmRaised |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.25 |

| Property name | Value |
|-----------------------|--|
| Default severity | minor |
| Source stream | main |
| Message format string | MRP attribute table utilization of service <i>\$svclD\$</i> (customer <i>\$custId\$</i>) 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 1654: *svcTlsProxyArpDupClear* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2347 |
| Event name | svcTlsProxyArpDupClear |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.57 |
| Default severity | minor |
| Source stream | main |
| Message format string | A duplicate proxy ARP entry <i>\$svcTlsProxyArpIpAddr\$</i> is cleared in service <i>\$svclD\$</i> |
| 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 1655: *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 <i>\$svcNotifTlsProxyMacAddr\$</i> for entry IP <i>\$svcTlsProxyArpIpAddr\$</i> MAC <i>\$svcTlsProxyArpMacAddr\$</i> in service <i>\$svclId\$</i> |
| Cause | The <i>svcTlsProxyArpDupDetect</i> 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 1656: *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 <i>\$svclId\$</i> has proxy ARP entries below 90% of the per-service limit |

| Property name | Value |
|---------------|--|
| 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 1657: svcTlsProxyArpSvcHiUsgSet properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2360 |
| Event name | svcTlsProxyArpSvcHiUsgSet |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.70 |
| Default severity | minor |
| Source stream | main |
| Message format string | Service <i>\$svcId\$</i> 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 1658: *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 1659: *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. |

| Property name | Value |
|---------------|---|
| Effect | 95% of the system proxy ARP entries limit is reached. |
| Recovery | None needed. |

76.136 svcTlsProxyArpUnauthorizedIP

Table 1660: svcTlsProxyArpUnauthorizedIP properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$svcTlsProxyArpIpAddr\$</i> in service <i>\$svcid\$</i> |
| Cause | The svcTlsProxyArpUnauthorizedIP notification is generated when an attempt to create a unauthorized proxy ARP entry IP was made. |
| Effect | Restrict unauthorized ARP requests. |
| Recovery | None needed. |

76.137 svcTlsProxyNdDupClear

Table 1661: svcTlsProxyNdDupClear properties

| Property name | Value |
|------------------|-----------------------|
| Application name | SVC MGR |
| Event ID | 2349 |
| Event name | svcTlsProxyNdDupClear |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.59 |
| Default severity | minor |
| Source stream | main |
| Message format string | A duplicate proxy ND entry <i>\$svcTIsProxyNdIpAddr\$</i> is cleared in service <i>\$svclId\$</i> |
| Cause | The svcTIsProxyNdDupDetect 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 svcTIsProxyNdDupDetect

Table 1662: *svcTIsProxyNdDupDetect* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2348 |
| Event name | svcTIsProxyNdDupDetect |
| 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 <i>\$svcNotifTIsProxyMacAddr\$</i> for entry IP <i>\$svcTIsProxyArpIpAddr\$</i> MAC <i>\$svcTIsProxyArpMacAddr\$</i> in service <i>\$svclId\$</i> |
| Cause | The svcTIsProxyNdDupDetect 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 1663: 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 1664: 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 |

| Property name | Value |
|-----------------------|---|
| Message format string | Service <i>\$svcid\$</i> has proxy ND entries in excess of 95% of the per-service limit |
| Cause | The <i>svcTlsProxyNdSvcHiUsgSet</i> 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 1665: *svcTlsProxyNdSysHiUsgClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2363 |
| Event name | <i>svcTlsProxyNdSysHiUsgClr</i> |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB. <i>svcTraps.73</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | The proxy ND entries is below 90% of the system limit |
| Cause | The <i>svcTlsProxyNdSysHiUsgClr</i> 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 1666: *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 1667: *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 <i>\$svcTlsProxyArplpAddr\$</i> in service <i>\$svclId\$</i> |
| Cause | The svcTlsProxyNdUnauthorizedIP notification is generated when an attempt to create a unauthorized proxy ND entry IP was made. |

| Property name | Value |
|---------------|---|
| Effect | Restrict unauthorized neighbor recovery requests. |
| Recovery | None needed. |

76.144 svcTlsSiteDesigFwdrChg

Table 1668: 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 \$svcTlsSiteIdDesignatedFwdr\$ the designated-forwarder |
| Cause | Designated-Forwarder status of the BGP multi-homing site associated with this service has changed. |
| Effect | N/A |
| Recovery | N/A |

76.145 svcTlsVTEPEgrVniSvcHiUsgAlarmClr

Table 1669: svcTlsVTEPEgrVniSvcHiUsgAlarmClr properties

| Property name | Value |
|------------------|----------------------------------|
| Application name | SVCMGR |
| Event ID | 2340 |
| Event name | svcTlsVTEPEgrVniSvcHiUsgAlarmClr |

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.51 |
| Default severity | minor |
| Source stream | main |
| Message format string | Service <i>\$svcid\$</i> 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 1670: svcTlsVTEPEgrVniSvcHiUsgAlarmSet properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2339 |
| Event name | svcTlsVTEPEgrVniSvcHiUsgAlarmSet |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.50 |
| Default severity | minor |
| Source stream | main |
| Message format string | Service <i>\$svcid\$</i> 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 1671: 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 1672: 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 |

| Property name | Value |
|-----------------------|---|
| 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 1673: svcTlsVTEPHiUsageAlarmCleared properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2336 |
| Event name | svcTlsVTEPHiUsageAlarmCleared |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.47 |
| Default severity | minor |
| Source stream | main |
| 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 1674: *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 1675: *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 <i>\$svclD\$</i> , vpn <i>\$svcVpnId\$</i> , vxlan instance <i>\$svcVxlanInstancelD\$</i> 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, |

| Property name | Value |
|---------------|---|
| | drops to the watermark specified by the object svcTIsFdbTableFullLowWatermark. |
| Effect | The number of MAC addresses stored in the FDB drops below svcTIsFdbTableFullLowWatermark. |
| Recovery | None needed. |

76.152 svcTIsVxInstMacAdrLimitAlrmRsd

Table 1676: svcTIsVxInstMacAdrLimitAlrmRsd properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2600 |
| Event name | svcTIsVxInstMacAdrLimitAlrmRsd |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.94 |
| Default severity | minor |
| Source stream | main |
| Message format string | Mac address limit for service <i>\$svcid\$</i> , vpn <i>\$svcVpnId\$</i> , vxlan instance <i>\$svcVxlanInstanceld\$</i> reached the high watermark |
| Cause | The trap svcTIsVxInstMacAdrLimitAlrmRsd 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 svcTIsFdbTableFullHighWatermark. |
| Effect | The number of MAC addresses stored in the FDB, increases to reach the watermark specified by svcTIsFdbTableFullHighWatermark. |
| Recovery | None needed. |

76.153 svcTIsVxInstReplicatorChgd

Table 1677: svcTlsVxInstReplicatorChgd properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 \$svcTlsVxInstVTEPAddress\$, 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 1678: svcTlsVxInstVTEPEgrVniStateChgd properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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\$) |

| 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. |

76.155 svcVIISiteDesigFwdrChg

Table 1679: svcVIISiteDesigFwdrChg properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVCMGR |
| Event ID | 2545 |
| Event name | svcVIISiteDesigFwdrChg |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.41 |
| Default severity | warning |
| Source stream | main |
| Message format string | Service-id <i>\$svcId\$</i> site <i>\$svcVIISiteIdName\$</i> is <i>\$svcVIISiteIdDesignatedFwdr\$</i> the designated-forwarder |
| Cause | Designated-Forwarder status of the BGP multi-homing site associated with this service has changed. |
| Effect | The new designated forwarder will be used to forward traffic. |
| Recovery | None needed. |

76.156 svcVxlanEvpnMplsDestSysHiUsgClr

Table 1680: svcVxlanEvpnMplsDestSysHiUsgClr properties

| Property name | Value |
|------------------|--------|
| Application name | SVCMGR |

| Property name | Value |
|----------------------------------|--|
| 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 1681: svcVxlanEvpnMplsDestSysHiUsgSet properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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. |

| Property name | Value |
|---------------|---|
| Effect | 95% of the system EVPN destinations(MPLS and VXLAN) limit is reached. |
| Recovery | None needed. |

76.158 tmnxEndPointTxActiveChanged

Table 1682: 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\$ |
| 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 1683: tmnxIpTunnelOperRemIpChg properties

| Property name | Value |
|------------------|--------|
| Application name | SVCMGR |
| Event ID | 2547 |

| Property name | Value |
|----------------------------------|--|
| 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 <i>\$tmnxIpTunnelName\$</i> has changed to <i>\$tmnxIpTunnelOperRemIpAddr\$</i> |
| Cause | The tmnxIpTunnelOperRemIpChg notification is generated when there is a change in operational remote address 'tmnxIpTunnelOperRemIpAddr' 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 1684: tmnxIpTunnelOperStateChange properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxIpTunnelName\$</i> on service <i>\$svcId\$</i> and SAP <i>\$sapEncapValue\$</i> , admin state: <i>\$tmnxIpTunnelAdminState\$</i> , oper state: <i>\$tmnxIpTunnelOperState\$</i> , oper flags: <i>\$tmnxIpTunnelOperFlags\$</i> |
| 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. |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

76.161 tmnxPfcPAssocPathMgmtStateChgd

Table 1685: tmnxPfcPAssocPathMgmtStateChgd properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2604 |
| Event name | tmnxPfcPAssocPathMgmtStateChgd |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.53 |
| Default severity | warning |
| Source stream | main |
| Message format string | PFCP association <i>\$tmnxPfcPAssocName\$</i> path management state changed to <i>\$tmnxPfcPAssocPathMgmtState\$</i> - <i>\$tmnxPfcPAssocRestartReason\$</i> |
| 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 1686: tmnxSapMRtCpeChkStatusChange properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |
| Event ID | 2619 |

| Property name | Value |
|----------------------------------|--|
| 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 <i>\$tmnxSapMRtCpeChkMRtAddr\$/\$tmnxSapMRtCpeChkMRtPrefixLen\$</i> is now <i>\$tmnxSapMRtCpeChkStatus\$</i> (service= <i>\$svclD\$</i> sap= <i>\$sapEncapValue\$</i> host-ip= <i>\$tmnxSapMRtCpeChkHostAddr\$</i> host-mac= <i>\$tmnxSapMRtCpeChkHostMacAddress\$</i>) |
| Cause | The CPE with address <i>tmnxSapMRtCpeChkAddr</i> becomes unreachable or reachable again according to the conditions specified in the <i>tmnxSapMRtCpeChkEntry</i> and while the value of <i>tmnxSapMRtCpeChkEnableLog</i> 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 <i>tmnxSapMRtCpeChkEntry</i> configuration. |
| Recovery | Depending on the situation. If the CPE is reachable via another system, no recovery may be necessary. |

76.163 tmnxSapStpExcepCondStateChng

Table 1687: *tmnxSapStpExcepCondStateChng* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$svclD\$</i> (customer <i>\$custId\$</i>) on SAP <i>\$sapEncapValue\$</i> has changed to <i>\$sapTIsStpException\$</i> |

| Property name | Value |
|---------------|---|
| Cause | The tmnxSapStpExcepCondStateChng notification is generated when the value of the object sapTIsStpException has changed, i.e. when the exception condition changes on the indicated SAP. |
| Effect | N/A |
| Recovery | N/A |

76.164 tmnxStpRootGuardViolation

Table 1688: tmnxStpRootGuardViolation properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVCMGR |
| Event ID | 2043 |
| Event name | tmnxStpRootGuardViolation |
| SNMP notification prefix and OID | TIMETRA-SAP-MIB.tstpTraps.35 |
| Default severity | minor |
| Source stream | main |
| Message format string | A root-guard violation is detected for service <i>\$svcl</i> on SAP <i>\$sap EncapValue</i> |
| 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 1689: *tmnxSubAcctPlyFailure* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2503 |
| Event name | tmnxSubAcctPlyFailure |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.4 |
| Default severity | warning |
| Source stream | main |
| Message format string | Radius accounting policy <i>\$tmnxSubAcctPlyName\$</i> failure - <i>\$tmnxSubAcctPlyFailureReason\$</i> . |
| 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 tmnxSubAcctPlyRadSerOperStatChg

Table 1690: *tmnxSubAcctPlyRadSerOperStatChg* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2506 |
| Event name | tmnxSubAcctPlyRadSerOperStatChg |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.7 |
| Default severity | minor |
| Source stream | main |
| Message format string | Subscriber Accounting RADIUS server <i>\$tmnxSubAcctPlyRadServAddr\$</i> operational status changed to <i>\$tmnxSubAcctPlyRadServOperState\$</i> . |

| Property name | Value |
|---------------|---|
| 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 1691: tmnxSubAuthPlcyRadSerOperStatChg properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2505 |
| Event name | tmnxSubAuthPlcyRadSerOperStatChg |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.6 |
| Default severity | minor |
| Source stream | main |
| Message format string | Subscriber Authentication RADIUS server <i>\$tmnxSubAuthPlcyRadServ Address\$</i> operational status changed to <i>\$tmnxSubAuthPlcyRadServ OperState\$</i> . |
| 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 1692: *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 <i>\$tmnxSubBrgId\$</i> 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 tmnxSubBrgCvInitFailed

Table 1693: *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 <i>\$tmnxSubBrgId\$</i> using IP address <i>\$tmnxSubNotifIpAddr\$</i> |
| Cause | The system issues the tmnxSubBrgCvInitFailed notification when it does not have enough resources to start connectivity verification for a |

| Property name | Value |
|---------------|---|
| | Bridged Residential Gateway (BRG) identified by <code>tmnxSubBrgId</code> , using the IP address <code>tmnxSubNotifIpAddr</code> in the virtual router instance with identifier <code>vRtrID</code> . 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 rely on the BRG host activity to determine if the BRG is connected. |
| Recovery | Not required. |

76.170 `tmnxSubBrgDeleted`

Table 1694: `tmnxSubBrgDeleted` properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVCMGR |
| Event ID | 2565 |
| Event name | <code>tmnxSubBrgDeleted</code> |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB. <code>tmnxSubscriberNotifications.39</code> |
| Default severity | warning |
| Source stream | main |
| Message format string | The Bridged Residential Gateway with identifier <code>\$tmnxSubBrgId\$</code> has been removed from the system. |
| Cause | The system issues the <code>tmnxSubBrgDeleted</code> notification when it destroys a conceptual row in the <code>tmnxSubBrgTable</code> . 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 1695: *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 <i>\$tmnxSubBrgId\$</i> - <i>\$tmnxSubRadiusSubAuthReason\$</i> |
| Cause | The <i>tmnxSubBrgRadiusAuthError</i> 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 1696: *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 <i>\$tmnxSubBrgId\$</i> - <i>\$tmnxSubRadiusCoAReason\$</i> |

| Property name | Value |
|---------------|---|
| Cause | The tmnxSubBrgRadiusCoaError notification indicates that the system was unable to process a Radius Change of Authorization (CoA) request for a Bridged Residential Gateway (BRG). |
| Effect | All hosts associated with the BRG use outdated parameters. |
| Recovery | Depends on the details of the failure. |

76.173 tmnxSubBrgRadiusProxyAuthError

Table 1697: tmnxSubBrgRadiusProxyAuthError properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2574 |
| Event name | tmnxSubBrgRadiusProxyAuthError |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.47 |
| Default severity | warning |
| Source stream | main |
| Message format string | Could not proxy-authenticate the Bridged Residential Gateway \$tmnxSubBrgId\$ - \$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 1698: *tmnxSubBrgRadiusUpdateIpoESeFail* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubBrgId\$</i> to the IPoE session with MAC <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | The system issues the <i>tmnxSubBrgRadiusUpdateIpoESeFail</i> 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 <i>tmnxSubBrgId</i> , the IPoE session by <i>svclId</i> , <i>sapPortId</i> , <i>sapEncapValue</i> and <i>tmnxSubNotifMacAddr</i> . More details about the failure are in <i>tmnxSubAdditionalInfo</i> . |
| Effect | A particular IPoE session has outdated parameters. |
| Recovery | Depends on the details of the failure. |

76.175 *tmnxSubBrgSessionLimitReached*

Table 1699: *tmnxSubBrgSessionLimitReached* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2570 |
| Event name | tmnxSubBrgSessionLimitReached |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.44 |
| Default severity | warning |

| Property name | Value |
|-----------------------|--|
| Source stream | main |
| Message format string | Bridged Residential Gateway <i>\$tmnxSubBrgId\$</i> exceeded its limit of 128 IPoE sessions |
| Cause | The system issues the <i>tmnxSubBrgSessionLimitReached</i> notification when this system fails to create an IPoE session associated with the Bridged Residential Gateway identified by <i>tmnxSubBrgId</i> 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 tmnxSubCupsUplfCreationFailed

Table 1700: *tmnxSubCupsUplfCreationFailed* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2603 |
| Event name | <i>tmnxSubCupsUplfCreationFailed</i> |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB. <i>tmnxSubscriberNotifications.52</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Could not create <i>\$iesIfType\$</i> interface <i>\$iesIfName\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | A failure occurs while the CUPS User Plane tries to create an interface. The object <i>tmnxSubAdditionalInfo</i> 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 1701: tmnxSubCupsUpSapCreationFailed properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1702: tmnxSubDhcpOverloadDetected properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2572 |
| Event name | tmnxSubDhcpOverloadDetected |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.46 |
| Default severity | warning |

| Property name | Value |
|-----------------------|---|
| Source stream | main |
| Message format string | DHCP message processing overload detected: <i>\$tmnxSubSysChass DhcpOverload\$</i> |
| Cause | The system issues the <code>tmnxSubDhcpOverloadDetected</code> 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 1703: *tmnxSubHostInconsistentAtmTdOvr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2536 |
| Event name | <code>tmnxSubHostInconsistentAtmTdOvr</code> |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB. <code>tmnxSubscriberNotifications.20</code> |
| Default severity | warning |
| Source stream | main |
| Message format string | Inconsistent ATM traffic descriptor given by AAA server for a host of subscriber <i>\$tmnxSubHostInfoV2SubIdent\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1704: tmnxSubHostInfoConflict properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubNotifMacAddr\$</i> of subscriber <i>\$tmnxSubIdent\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1705: tmnxSubHostLcktLimitReached properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2548 |
| Event name | tmnxSubHostLcktLimitReached |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.22 |
| Default severity | minor |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | Maximum number of <i>\$tmnxSubAdditionalInfo\$</i> 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 1706: tmnxSubHostLcktSapLimitReached properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2549 |
| Event name | tmnxSubHostLcktSapLimitReached |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.23 |
| Default severity | minor |
| Source stream | main |
| Message format string | Maximum number of <i>\$tmnxSubLcktPlcyMaxLcktHosts\$</i> locked out hosts is reached on host <i>\$tmnxSubNotifMacAddr\$</i> . |
| 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 1707: *tmnxSubInfoEgrAggRateLimitLowReq* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubInfoSubIdent\$</i> : attempt to limit egress aggregate rate below reserved minimum (<i>\$tmnxSubAdditionalInfo\$</i>) - <i>\$tmnxSubInfoEgrAggRateLimitLow\$</i> |
| 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 tmnxSublpoelInvalidCidRidChange

Table 1708: *tmnxSublpoelInvalidCidRidChange* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2555 |
| Event name | tmnxSublpoelInvalidCidRidChange |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.29 |
| Default severity | warning |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | IPoE session CID/RID change failure for host with MAC address <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1709: *tmnxSubIpoeInvalidSessionKey* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2554 |
| Event name | tmnxSubIpoeInvalidSessionKey |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.28 |
| Default severity | warning |
| Source stream | main |
| Message format string | IPoE session key failure for host with MAC address <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1710: *tmnxSublpoeMigrHostDeleted* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2559 |
| Event name | tmnxSublpoeMigrHostDeleted |
| 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 <i>\$tmnxSubNotifIpAddr\$</i> / <i>\$tmnxSubNotifPrefixLength\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 tmnxSublpoePersistenceRecovery

Table 1711: *tmnxSublpoePersistenceRecovery* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2557 |
| Event name | tmnxSublpoePersistenceRecovery |
| 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 <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | The system is still recovering from persistence. |

| Property name | Value |
|---------------|---|
| Effect | The system cannot setup the IPoE session. |
| Recovery | No recovery is required on this system. |

76.188 tmnxSublpoeSessionBrgNotAuth

Table 1712: tmnxSublpoeSessionBrgNotAuth properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2575 |
| Event name | tmnxSublpoeSessionBrgNotAuth |
| 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 <i>\$tmnxSubBrgId\$</i> with MAC address <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 tmnxSublpoeSessionLimitReached

Table 1713: tmnxSublpoeSessionLimitReached properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |
| Event ID | 2556 |

| Property name | Value |
|----------------------------------|---|
| 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 <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1714: *tmnxSubIpoeWppRegistrationFailed* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | The cause is given in <i>tmnxSubAdditionalInfo</i> . |
| Effect | The system cannot setup the IPoE session. |
| Recovery | No recovery is required on this system. |

76.191 tmnxSubMcsRelatedProblem

Table 1715: 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: <i>\$tmnxSubMcsRelatedProblemDescr\$</i> |
| 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 1716: 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 |

| Property name | Value |
|-----------------------|--|
| Message format string | Could not create host IP <i>\$tmnxSubNotifIpAddr\$</i> MAC <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | A failure occurs while trying to create a managed host. The object <i>tmnxSubAdditionalInfo</i> 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 1717: *tmnxSubMngdHostOverride* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2561 |
| Event name | tmnxSubMngdHostOverride |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.35 |
| Default severity | warning |
| Source stream | main |
| Message format string | Existing managed host IP <i>\$tmnxSubMngdHostIpAddr\$</i> MAC <i>\$tmnxSubMngdHostMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> overridden - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | The <i>tmnxSubMngdHostOverride</i> 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 tmnxSubPIBndFailed

Table 1718: tmnxSubPIBndFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVCMGR |
| Event ID | 2563 |
| Event name | tmnxSubPIBndFailed |
| 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 <i>\$tmnxSubNotifName\$</i> for the host with MAC <i>\$tmnxSubNotifMacAddr\$</i> on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | The system issues the tmnxSubPIBndFailed 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 1719: tmnxSubPysrosExec properties

| Property name | Value |
|------------------|-------------------|
| Application name | SVCMGR |
| Event ID | 2627 |
| Event name | tmnxSubPysrosExec |

| Property name | Value |
|----------------------------------|--|
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.59 |
| Default severity | warning |
| Source stream | main |
| Message format string | Run <i>#\$smRunIndex\$</i> of script-policy " <i>#\$smLaunchName\$</i> " created by owner " <i>#\$smLaunchOwner\$</i> " invoked. Triggered by subscriber <i>\$tmnxSubIdent\$</i> [svc: <i>\$svcName\$</i> , sap: <i>\$sapEncapValue\$</i> , mac: <i>\$tmnxSubNotifMacAddr\$</i> , sid: <i>\$tmnxSubNotifPppoeSessionId\$</i> circuit-id: <i>\$tmnxSubNotifCircuitId\$</i> remote-id: <i>\$tmnxSubNotifRemoteId\$</i>] |
| 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 1720: tmnxSubPysrosExecFail properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2628 |
| Event name | tmnxSubPysrosExecFail |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.60 |
| Default severity | warning |
| Source stream | main |
| Message format string | Failed to invoke script-policy " <i>#\$smLaunchName\$</i> " created by owner " <i>#\$smLaunchOwner\$</i> ": <i>\$tmnxSubAdditionalInfo\$</i> . Triggered by subscriber <i>\$tmnxSubIdent\$</i> [svc: <i>\$svcName\$</i> , sap: <i>\$sapEncapValue\$</i> , mac: <i>\$tmnxSubNotifMacAddr\$</i> , sid: <i>\$tmnxSubNotifPppoeSessionId\$</i> circuit-id: <i>\$tmnxSubNotifCircuitId\$</i> remote-id: <i>\$tmnxSubNotifRemoteId\$</i>] |
| Cause | The system encountered a runtime failure while executing a pySROS script. |
| Effect | The effect depends on the contents of the script. |

| Property name | Value |
|---------------|--|
| Recovery | Recovery depends on the contents of the script and on the failure cause. |

76.197 tmnxSubRadiusCoaNatFwdFailed

Table 1721: tmnxSubRadiusCoaNatFwdFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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. |
| 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 1722: *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 <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> from a Radius server: <i>\$tmnxSubRadiusCoAReason\$</i> |
| 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 1723: *tmnxSubRadSapDisconnectError* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVCMGR |
| Event ID | 2509 |
| Event name | tmnxSubRadSapDisconnectError |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.8 |
| Default severity | warning |
| Source stream | main |
| Message format string | Problem encountered in Subscriber Management, while processing a Disconnect request on SAP <i>\$sapEncapValue\$</i> in service <i>\$svclId\$</i> from a Radius server: <i>\$tmnxSubRadiusDisconnectReason\$</i> |

| Property name | Value |
|---------------|---|
| Cause | The system was unable to process a Disconnect request from a Radius server. |
| Effect | N/A |
| Recovery | N/A |

76.200 tmnxSubRadSapSubAuthError

Table 1724: tmnxSubRadSapSubAuthError properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> : <i>\$tmnxSubRadiusSubAuthReason\$</i> |
| Cause | The system encountered a problem while trying to authenticate a subscriber. |
| Effect | N/A |
| Recovery | N/A |

76.201 tmnxSubRadSdpBndCoAError

Table 1725: tmnxSubRadSdpBndCoAError properties

| Property name | Value |
|------------------|---------|
| Application name | SVC MGR |

| Property name | Value |
|----------------------------------|--|
| 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> from a Radius server: <i>\$tmnxSubRadiusCoAReason\$</i> |
| 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 1726: *tmnxSubRadSdpBndDisconnectError* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2510 |
| Event name | tmnxSubRadSdpBndDisconnectError |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.9 |
| Default severity | warning |
| Source stream | main |
| Message format string | Problem encountered in Subscriber Management, while processing a Disconnect request on SDP Bind <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> from a Radius server: <i>\$tmnxSubRadiusDisconnectReason\$</i> |
| Cause | The system was unable to process a Disconnect request from a Radius server. |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

76.203 tmnxSubRadSdpBndSubAuthError

Table 1727: tmnxSubRadSdpBndSubAuthError properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$sdpBindId\$</i> in service <i>\$svclId\$</i> : <i>\$tmnxSubRadiusSubAuthReason\$</i> |
| 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 1728: tmnxSubscriberCreated properties

| Property name | Value |
|------------------|-----------------------|
| Application name | SVC MGR |
| Event ID | 2500 |
| Event name | tmnxSubscriberCreated |

| Property name | Value |
|----------------------------------|---|
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.1 |
| Default severity | warning |
| Source stream | main |
| Message format string | Subscriber <i>\$tmnxSubIdent\$</i> 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 1729: tmnxSubscriberDeleted properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubIdent\$</i> 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 1730: *tmnxSubscriberRenamed* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 <i>\$tmnxOldSubIdent\$</i> has been renamed to <i>\$tmnxNewSubIdent\$</i> . |
| 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 1731: *tmnxSubSlaacOverride* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 (<i>\$tmnxSubSlaacPfx\$</i> / <i>\$tmnxSubSlaacPfxLen\$</i> , <i>\$tmnxSubSlaacMacAddr\$</i>) on SAP <i>\$tmnxSubSlaacEncapValue\$</i> in service <i>\$svclD\$</i> overridden by DHCP6 lease-state (<i>\$svcDhcpLeaseCiAddr\$</i> / <i>\$svcDhcpLeaseCiAddrMaskLen\$</i> , <i>\$svcDhcpLeaseNextHopMacAddr\$</i>) |

| Property name | Value |
|---------------|---|
| 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 1732: 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 <i>\$sapEncapValue\$</i> in service <i>\$svcId\$</i> - <i>\$tmnxSubAdditionalInfo\$</i> |
| 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 1733: tmnxSubStatsResourceLimitReached properties

| Property name | Value |
|------------------|--------|
| Application name | SVCMGR |

| Property name | Value |
|----------------------------------|--|
| 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 <i>\$tmnxSubSysChassStatsUsed\$</i> subscribers with accumulated statistics and is above/below its limit of <i>\$tmnxSubNotifNumber\$</i> |
| 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, tmnxSubStatsEgrQTable and tmnxSubStatsIngTable. The limit may depend on the characteristics of the node. The actual limit is indicated in the tmnxSubNotifNumber 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 1734: tmnxSubSVlanStatsReachedMaximum properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2577 |
| Event name | tmnxSubSVlanStatsReachedMaximum |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.50 |

| Property name | Value |
|-----------------------|--|
| Default severity | warning |
| Source stream | main |
| Message format string | The number of entries in the Subscriber VLAN statistics table (<i>\$tmnxSubSVlanStatsNumEntries\$</i>) is <i>\$tmnxSubNotifTruthValue\$</i> its maximum. |
| Cause | The <i>tmnxSubSVlanStatsReachedMaximum</i> notification indicates if the object <i>tmnxSubSVlanStatsNumEntries</i> is at its maximum value. The object <i>tmnxSubSVlanStatsNumEntries</i> indicates the number of conceptual rows in the <i>tmnxSubSVlanStatsTable</i> . When the value of <i>tmnxSubNotifTruthValue</i> is equal to 'true', the object <i>tmnxSubSVlanStatsNumEntries</i> is at its maximum value. When it is 'false', the value of <i>tmnxSubSVlanStatsNumEntries</i> has decreased below its maximum value again. |
| Effect | For any additional subscriber traffic flows, no new entry will be created in the <i>tmnxSubSVlanStatsTable</i> , and no such statistics will be available. |
| Recovery | No recovery required. |

76.211 tmnxSubSysChassMemoryUsageHi

Table 1735: *tmnxSubSysChassMemoryUsageHi* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2551 |
| Event name | <i>tmnxSubSysChassMemoryUsageHi</i> |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB. <i>tmnxSubscriberNotifications.26</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | The subscriber management's memory usage high status in chassis <i>\$tmnxChassisIndex\$</i> changed to <i>\$tmnxSubSysChassMemoryUsageHigh\$</i> . |
| Cause | The <i>tmnxSubSysChassMemoryUsageHi</i> notification is sent when the memory usage by subscriber management on this system reaches |

| Property name | Value |
|---------------|---|
| | 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 1736: tmnxSubUserCategoryError properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubNotifIpAddr\$</i> with MAC address <i>\$tmnxSubNotifMacAddr\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svclId\$</i> . Subscriber: <i>\$tmnxSubIdent\$</i> . SLA Profile: <i>\$tmnxSubNotifSLAProfName\$</i> . Category Map name: <i>\$tmnxSubNotifApCMapName\$</i> . Category name: <i>\$tmnxSubNotifApCategoryName\$</i> . More info: <i>\$tmnxSubAdditionalInfo\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

76.213 tmnxSubUserCategoryOutOfCredit

Table 1737: *tmnxSubUserCategoryOutOfCredit* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| 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 <i>\$tmnxSubNotifIpAddr\$</i> with MAC address <i>\$tmnxSubNotifMacAddr\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svclId\$</i> . Subscriber: <i>\$tmnxSubIdent\$</i> . SLA Profile: <i>\$tmnxSubNotifSLAProfName\$</i> . Category Map name: <i>\$tmnxSubNotifApCMapName\$</i> . Category name: <i>\$tmnxSubNotifApCategoryName\$</i> . |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

76.214 tmnxSubUserCategoryRefreshCredit

Table 1738: *tmnxSubUserCategoryRefreshCredit* properties

| Property name | Value |
|----------------------------------|---|
| Application name | SVC MGR |
| Event ID | 2529 |
| Event name | tmnxSubUserCategoryRefreshCredit |
| SNMP notification prefix and OID | TIMETRA-SUBSCRIBER-MGMT-MIB.tmnxSubscriberNotifications.15 |
| Default severity | minor |
| Source stream | main |
| Message format string | The credit refresh has been initiated for host <i>\$tmnxSubNotifIpAddr\$</i> with MAC address <i>\$tmnxSubNotifMacAddr\$</i> on SAP: <i>\$sapEncapValue\$</i> , service: <i>\$svclId\$</i> . Subscriber: <i>\$tmnxSubIdent\$</i> . SLA Profile: <i>\$tmnx</i> |

| Property name | Value |
|---------------|--|
| | <i>SubNotifSLAProfName</i> \$. Category Map name: <i>\$tmnxSubNotifApCMapName</i> \$. Category name: <i>\$tmnxSubNotifApCategoryName</i> \$. |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

76.215 tmnxSubVSubnetHostsDeleted

Table 1739: 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 <i>\$tmnxSubInfoSubIdent</i> \$ in service <i>\$svcId</i> \$ because of a new gateway IP/subnet assignment <i>\$tmnxSubVSubnetDefRtrAddr</i> \$/ <i>\$tmnxSubVSubnetPrefixLength</i> \$ |
| 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 1740: *tmnxSvcSysFdbTableHighUsgClr* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| 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 = <i>\$tmnxSvcSysFdbAllocEntries\$</i> |
| 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 1741: *tmnxSvcSysFdbTableHighUsgSet* properties

| Property name | Value |
|----------------------------------|--|
| Application name | SVC MGR |
| Event ID | 2107 |
| Event name | tmnxSvcSysFdbTableHighUsgSet |
| SNMP notification prefix and OID | TIMETRA-SERV-MIB.svcTraps.90 |
| Default severity | minor |
| Source stream | main |
| Message format string | The system FDB table usage is above 95% of the system FDB table size, Current usage = <i>\$tmnxSvcSysFdbAllocEntries\$</i> |

| Property name | Value |
|---------------|--|
| 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 1742: 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 <i>\$userName\$</i> (<i>\$interface\$</i>) from <i>\$srcAddr\$</i> is taking longer than expected - <i>\$reason\$</i> . |
| 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 1743: 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 <i>\$regionName\$</i> by <i>\$userName\$</i> (<i>\$interface\$</i>) from <i>\$srcAddr\$</i> succeeded. |
| Cause | The mdCommitSucceeded event is generated when a commit succeeded. |
| Effect | The commit succeeded. |
| Recovery | No recovery is necessary. |

77.3 mdSaveCommitHistoryFailed

Table 1744: 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 | <i>\$regionName\$</i> commit history file write failed: <i>\$fileName\$</i> |
| 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 1745: 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 <i>\$tmnxPersistenceClient\$</i> - <i>\$tmnxPersistenceNotifyMsg\$</i> |
| 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 1746: 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 <i>\$tmnxPersistenceAffectedCpm\$</i> for <i>\$tmnxPersistencyClient\$</i> on device <i>\$tmnxPersistencyFileLocator\$</i> is re-opened. <i>\$tmnxPersistencyNotifyMsg\$</i> |
| 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 1747: *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 <i>\$tmnxPersistenceAffectedCpm\$</i> for <i>\$tmnxPersistencyClient\$</i> on device <i>\$tmnxPersistencyFileLocator\$</i> is closed. Persistency across system reboot is no longer guaranteed. <i>\$tmnxPersistencyNotifyMsg\$</i> |
| 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 1748: *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: <i>\$tmnxPersistencyNotifyMsg\$</i> |
| 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 1749: *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 <i>\$tmnxPersistenceAffectedCpm\$</i> for <i>\$tmnxPersistencyClient\$</i> on device <i>\$tmnxPersistencyFileLocator\$</i> has dropped below threshold level of 90 percent. <i>\$tmnxPersistencyNotifyMsg\$</i> |

| 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 1750: 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 <i>\$tmnxPersistenceAffectedCpm\$</i> for <i>\$tmnxPersistencyClient\$</i> on device <i>\$tmnxPersistencyFileLocator\$</i> has reached threshold level of 90 percent. <i>\$tmnxPersistencyNotifyMsg\$</i> |
| Cause | The persistencyFileSysThresRaised notification is generated when the filesystem reaches 90 percent occupation. |
| Effect | N/A |
| Recovery | N/A |

77.10 sbiBootConfig

Table 1751: 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: <i>\$sbiConfigStatus\$</i> . SNMP Persistent Indexes status: <i>\$sbiPersistStatus\$</i> . System configured with persistent indexes: <i>\$sbiPersistIndex\$</i> . |
| Cause | The configuration phase following a system reboot has completed. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

77.11 sbiBootConfigFailFileError

Table 1752: *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 <i>\$sbiBootConfigFailScript\$</i> |
| Cause | The bootup failed script file is not accessible. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

77.12 sbiBootConfigOKFileError

Table 1753: 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 <i>\$sbiBootConfigOKScript\$</i> |
| Cause | The bootup configuration OK script file was not accessible. |
| Effect | N/A |
| Recovery | No recovery is necessary. |

77.13 sbiBootMdReadCommitHistoryFailed

Table 1754: 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 | <i>\$regionName\$</i> commit history file read failed: <i>\$fileName\$</i> |
| 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 1755: 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: <i>\$sbiPersistIndex\$</i> . SNMP daemon administrative status: <i>\$sbiSnmpdAdminStatus\$</i> . SNMP daemon operational status: <i>\$sbiSnmpdOperStatus\$</i> . |
| 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 1756: 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 1757: 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 "\$smLaunchName\$" 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 1758: 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 <i>\$tmnxSmRunExtAuthType\$</i> operation completed with an exception: <i>\$smRunError\$</i> . Run # <i>\$smRunIndex\$</i> of script-policy " <i>\$smLaunchName\$</i> " created by owner " <i>\$smLaunchOwner\$</i> " was executed with the user account " <i>\$tmnxSmRunExtUserName\$</i> " |
| 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 1759: 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 <i>\$tmnxSmRunExtAuthType\$</i> operation completed with the result: <i>\$smRunResult\$</i> . Run # <i>\$smRunIndex\$</i> of script-policy " <i>\$smLaunchName\$</i> " created by owner " <i>\$smLaunchOwner\$</i> " was executed with the user account " <i>\$tmnxSmRunExtUserName\$</i> ". |
| 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 1760: 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 <i>\$sntp_ip_address\$</i> 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 1761: 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 1762: *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 1763: *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: <i>\$fileName\$</i> <i>\$reason\$</i> |
| 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 1764: 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: <i>\$fileName\$</i> |
| 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 1765: 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: <i>\$fileName\$ \$reason\$</i> |
| 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 1766: 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: <i>\$fileName\$</i> |
| Cause | Saving the configuration succeeded. |
| Effect | The configuration was saved. |
| Recovery | No recovery is necessary. |

77.26 ssiSaveIncrementConfigFailed

Table 1767: 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: <i>\$fileName\$ \$reason\$</i> |
| 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 1768: 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: <i>\$fileName\$</i> |
| Cause | An incremental configuration save was initiated. |
| Effect | The incremental configuration file was saved. |
| Recovery | No recovery is necessary. |

77.28 ssiSyncBootEnvFailed

Table 1769: 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 - <i>\$tmnxSyncFailure Reason\$</i> |
| 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 1770: 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 1771: 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 - <i>\$tmnxSyncFailureReason\$</i> |
| 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 1772: 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 1773: 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 - <i>\$tmnxSyncFailureReason</i> \$ |
| 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 1774: 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 1775: 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 - <i>\$tmnxSyncFailureReason\$</i> |

| 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 1776: 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 1777: *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 <i>\$stiDateAndTime\$</i> |
| 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 1778: *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 <i>\$stiDateAndTime\$</i> |
| 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 1779: 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 1780: 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 | <i>\$tmnxNotifyObjectName\$</i> 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 1781: *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 | <i>\$tmnxNotifyObjectName\$</i> 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 1782: 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 | <i>\$tmnxNotifyObjectName\$</i> 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 1783: 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 | <i>\$tmnxNotifyObjectName\$</i> 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 1784: *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 <i>\$tmnxSmRunExtAuthType\$</i> operation failed with a min delay violation error: Mindelay = <i>\$tmnxEhsHEntryMinDelay\$</i> is greater than Mindelay Interval: <i>\$tmnxEhsHEntryMinDelayInterval\$</i> . The script policy " <i>\$tmnxEhsHEntryScriptPlcyName\$</i> " created by the owner " <i>\$tmnxEhsHEntryScriptPlcyOwner\$</i> " was executed with cli-user account " <i>\$tmnxSmRunExtUserName\$</i> ". |
| 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 1785: 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 : " \$tmnxEhsHandlerDescription\$" was invoked by the cli-user account "\$tmnxSmRunExtUserName\$". |
| 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 1786: 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 <i>\$tmnxFtpFailureDestAddress\$</i> failed with error message <i>\$tmnxFtpFailureMsg\$</i> |
| Cause | A file transfer operation initiated by the FTP client failed. |
| Effect | N/A |
| Recovery | N/A |

77.46 tmnxLastSystemRebootAdmin

Table 1787: 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 <i>\$tmnxLastSystemRebootTime\$</i> by user <i>\$tmnxLastSystemRebootUser\$</i> from <i>\$tmnxLastSystemRebootUserAddress\$</i> |
| Cause | The tmnxLastSystemRebootAdmin notification is generated when the reason for the last system reboot (as indicated by tmnxLastSystemRebootReason) was 'admin (1)'. The tmnxLastSystemRebootAdmin notification is generated when the reason for the last system reboot (as indicated by tmnxLastSystemRebootReason) was 'admin (1)'. |
| Effect | No effect. |
| Recovery | No recovery is necessary. |

77.47 tmnxModuleMallocFailed

Table 1788: 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 <i>\$tmnxModuleMallocSize\$</i> bytes from module <i>\$tmnxMemoryModule\$</i> 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 1789: 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 <i>\$cpmSlotName\$</i> 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 1790: 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 <i>\$cpmSlotName\$</i> 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 1791: 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 <i>\$cpmSlotName\$</i> 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 1792: 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 <i>\$cpmSlotName\$</i> is in progress. |
| Cause | Synchronization of redundancy information onto the standby CPM was started. <i>tmnxChassisNotifyHwIndex</i> identifies the standby CPM. |
| Effect | N/A |
| Recovery | N/A |

77.52 tmnxRedStandbySyncLost

Table 1793: *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 <i>\$cpmSlotName\$</i> has been lost. |
| Cause | The active CPM lost communication with the standby CPM. |
| Effect | N/A |
| Recovery | N/A |

77.53 tmnxRedSwitchover

Table 1794: *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 <i>\$cpmSlotName\$</i> because <i>\$ssiRedFailoverReason\$</i> . |
| 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 1795: *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 <i>\$tmnxSmRunExtAuthType\$</i> operation failed with error: <i>\$smLaunchError\$</i> . The script policy " <i>\$tmnxEhsHEntryScriptPlyName\$</i> " created by the owner " <i>\$tmnxEhsHEntryScriptPlyOwner\$</i> " was executed with cli-user account " <i>\$tmnxSmRunExtUserName\$</i> " |
| 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 smScriptSource 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 smLaunchMaxRunning. |
| Effect | The result is indicated by incrementing the value of tmnxEhsHEntryStatsErrLaunch. |
| Recovery | No recovery is necessary. |

77.55 tmnxSnmpdStateChange

Table 1796: 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 <i>\$\$sbiSnmpdAdminStatus\$</i> and operational state is <i>\$\$sbiSnmpdOperStatus\$</i> . |
| 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 1797: *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 <i>\$sntpOperStatus\$</i> |
| Cause | There was a change in the operational state of SNTP. |
| Effect | N/A |
| Recovery | N/A |

77.57 tmnxSssiMismatch

Table 1798: *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 1799: 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 <i>\$tmnxNotifyObjectName\$</i> changed administrative state: <i>\$tmnxNotifyRowAdminState\$</i> , operational state: <i>\$tmnxNotifyRowOperState\$</i> |
| 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 1800: 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 <i>\$tmnxSysNotifAppStatsTime\$</i> for application <i>\$tmnxSysNotifAppStatsApplication\$</i> type <i>\$tmnxSysNotifAppStatsType\$</i> |
| 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 1801: 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 <i>\$tmnxSysNotifAppStatsTime\$</i> |

| Property name | Value |
|---------------|---|
| Cause | The system generates the <code>tmnxSysAppStatsWeekAvailable</code> notification when new rows are available in the <code>tmnxSysAppStatsWeekTable</code> . The value of <code>tmnxSysNotifAppStatsTime</code> indicates the time the system collected the values in the new rows. |
| Effect | None. |
| Recovery | No recovery is necessary. |

77.61 `tmnxSysBaseMacAddressNotSet`

Table 1802: `tmnxSysBaseMacAddressNotSet` properties

| Property name | Value |
|----------------------------------|--|
| Application name | SYSTEM |
| Event ID | 2067 |
| Event name | <code>tmnxSysBaseMacAddressNotSet</code> |
| 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 <code>\$tmnxChassisBaseMacAddress\$</code> which may not be unique. |
| Cause | The <code>tmnxSysBaseMacAddressNotSet</code> notification is generated once after the system boots up and the value of <code>sbiSystemBaseMacAddress</code> is all zeroes. |
| Effect | The system software is using the base MAC address specified in <code>tmnxChassisBaseMacAddress</code> which may not be unique. |
| Recovery | Configure <code>sbiSystemBaseMacAddress</code> to a value other than all zeroes. |

77.62 `tmnxSysDyingGasp`

Table 1803: *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 1804: *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 | <p>Possible messages:</p> <ul style="list-style-type: none"> 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 |
|---------------|--|
| | <ul style="list-style-type: none"> Processing of '<i>\$tmnxLogExecRollbackOpType\$</i>' configuration messages has completed with the result of '<i>\$tmnxSysExecResult\$</i>' |
| 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 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 | The effect is that the entry for the specified tmnxLogExecRollbackOpIndex 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 1805: 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: <ul style="list-style-type: none"> A CLI user has initiated an '<i>\$tmnxLogExecRollbackOpType\$</i>' operation to process the commands in the SR OS CLI file '<i>\$tmnxSysExecScript\$</i>' |

| Property name | Value |
|---------------|---|
| | <ul style="list-style-type: none"> 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 tmnxSysExecFinished 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 1806: 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 1807: 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 1808: 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 1809: 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 <i>\$tmnxSysMgmtIfWriteMode\$</i> 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 1810: *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 <i>\$tmnxSysMgmtIfWriteMode\$</i> 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 1811: *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 <i>\$tmnxSysMgmtIfWriteSwitchReason\$</i>) from <i>\$tmnxNotifySysMgmtIfOriginalMode\$</i> to <i>\$tmnxSysMgmtIfWriteMode\$</i> was initiated. |
| Cause | The <i>tmnxSysMgmtIfModeChangeStart</i> 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 1812: *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 <i>\$tmnxSysFileErrorType\$</i> file <i>\$fileName\$</i> |

| 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 1813: 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 <i>\$fileName\$</i> 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 1814: *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 <i>\$fileName\$ \$result\$</i> |
| Cause | The tmnxSysRollbackFileDeleteStatus notification is generated upon the completion of a rollback file delete as specified by tmnxSysRollbackIndex and tmnxSysRollbackFileType. |
| Effect | The result is indicated by the value of tmnxSysRollbackFileDeleteResult. |
| 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 1815: *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 <i>\$fileName\$</i> 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 1816: 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 <i>\$fileName\$</i> <i>\$result\$</i> |
| Cause | The tmnxSysRollbackSaveStatusChange notification is generated upon the completion of a rollback save as specified by tmnxSysRollbackFileType. |
| 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 1817: *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 <i>\$fileName\$</i> started |
| Cause | The tmnxSysRollbackStarted notification is generated when the user initiates a revert of the rollback checkpoint file specified by tmnxSysRollbackIndex 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 1818: *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 <i>\$fileName\$</i> <i>\$result\$</i> |
| 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 1819: 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 1820: *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 1821: *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 fabric 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 1822: 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 1823: *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 | <p>Possible messages:</p> <ul style="list-style-type: none"> • Dropped notification <i>\$tmnxDroppedTrapName\$</i> for <i>\$tmnxDroppedTrapEntryName\$</i> because of <i>\$tmnxTrapDroppedReasonCode\$</i> • Dropped notification <i>\$tmnxDroppedTrapName\$</i> for <i>\$tmnxDroppedTrapEntryName\$</i> because of <i>\$tmnxTrapDroppedReasonCode\$</i> - <i>\$tmnxTrapDroppedCount\$</i> traps dropped |
| Cause | <p>A <i>tmnxTrapDropped</i> notification is generated when a trap is dropped for the reason specified by the reason code. The <i>tmnxTrapDroppedEntryID</i> identifies the table entry associated with the dropped trap. A nonzero value of the object <i>tmnxTrapDroppedCount</i> indicates the number of traps dropped for the current flow of traps, identified by the values of <i>tmnxDroppedTrapID</i>, <i>tmnxTrapDroppedReasonCode</i> and <i>tmnxTrapDroppedEntryID</i>.</p> |
| Effect | N/A |
| Recovery | N/A |

78 TLS

78.1 tmnxTlsFailure

Table 1824: 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 <i>\$tmnxTlsAppId\$</i> <i>\$tmnxTlsRole\$</i> router instance <i>\$tmnxTlsVRtrID\$</i> source address <i>\$tmnxTlsLocalAddr\$</i> sourcePort <i>\$tmnxTlsLocalPort\$</i> destination address <i>\$tmnxTlsRemoteAddr\$</i> destinationPort <i>\$tmnxTlsRemotePort\$</i> failure reason <i>\$tmnxTlsFailureReason\$</i> |
| 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 1825: 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 <i>\$tmnxTlsAppId\$</i> <i>\$tmnxTlsRole</i> \$ router instance <i>\$tmnxTlsVRtrID\$</i> source address <i>\$tmnxTlsLocal</i> <i>Addr\$</i> sourcePort <i>\$tmnxTlsLocalPort\$</i> destination address <i>\$tmnxTls</i> <i>RemoteAddr\$</i> destinationPort <i>\$tmnxTlsRemotePort\$</i> tls state <i>\$tmnxTls</i> <i>ConnectionState\$</i> |
| 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 1826: 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 <i>\$tmnxTlsAppId\$</i> <i>\$tmnxTlsRole</i> \$ router instance <i>\$tmnxTlsVRtrID\$</i> source address <i>\$tmnxTlsLocalAddr</i> <i>\$</i> sourcePort <i>\$tmnxTlsLocalPort\$</i> destination address <i>\$tmnxTlsRemote</i> <i>Addr\$</i> destinationPort <i>\$tmnxTlsRemotePort\$</i> |

| 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 1827: 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 (\$vRtrTreeSidDBPlcyCPActiveInst\$) for p2mp-policy. |
| Cause | Generated when the active instance for a candidate-path changes from vRtrTreeSidDBPlcyCPOldActiveInst to vRtrTreeSidDBPlcyCPActiveInst; |
| Effect | Switching to the new active-instance for the candidate-path was successful. |
| Recovery | None required. |

79.2 vRtrTreeSidCdtPathChanged

Table 1828: 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 (<i>\$vRtrTreeSidDBPlcyOldCdtPathName\$</i>) to (<i>\$vRtrTreeSidDBPlcyCdtPathName\$</i>) for p2mp-policy . |
| Cause | Generated when the in-use candidate-path changes from vRtrTreeSidDBPlcyOldCdtPathName to vRtrTreeSidDBPlcyCdtPathName; |
| Effect | Switching to the new candidate-path was successful. |
| Recovery | None Required. |

79.3 vRtrTreeSidFailOverPriToStdBy

Table 1829: 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 <i>\$vRtrID\$</i> from primary PE <i>\$vRtrPimNgMvpnUMHPEAddr\$</i> to standby PE <i>\$vRtrPimNgMvpnUMHPEStandbyAddr\$</i> due to <i>\$vRtrTreeSidFailOverReasonCode\$</i> |
| 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 vRtrPimNgMvpnUMHPEAddrType 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 1830: 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 1831: 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 vRtrTreeSidDBRplPlyIncomingSid. |
| Effect | Programming of the replication-segment failed. |
| Recovery | Configuration change, using a different incoming-sid. |

79.6 vRtrTreeSidLabelRangeExhaustion

Table 1832: 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 1833: 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 vRtrTreeSidLabelRangeExhaustion is cleared. |
| Effect | System can accept new replication-segment configuration with pop and swap operation. |
| Recovery | None required. |

79.8 vRtrTreeSidRepSegResExhaustion

Table 1834: 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 vRtrTreeSid ResourceType 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 1835: 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 vRtrTreeSidTreeldAllocFailure

Table 1836: vRtrTreeSidTreeldAllocFailure properties

| Property name | Value |
|----------------------------------|--|
| Application name | TREE_SID |
| Event ID | 2004 |
| Event name | vRtrTreeSidTreeldAllocFailure |
| 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 1837: 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 <i>\$srcAddr\$</i> : <i>\$prompt\$ \$message\$</i> |
| 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 1838: 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 <i>\$srcAddr\$</i> . <i>\$message\$</i> : <i>\$prompt\$ \$command\$</i> |
| 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 1839: 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 <i>\$srcAddr\$</i> . <i>\$message\$</i> : <i>\$prompt\$ \$command\$</i> |
| 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 1840: 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 1841: 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 1842: 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 <i>\$srcAddr\$</i> 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 1843: 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 <i>\$srcAddr\$</i> attempted more than <i>\$maxAttempts\$</i> 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 1844: 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 1845: 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 <i>\$srcAddr\$</i> 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 1846: 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 <i>\$srcAddr\$</i> 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 1847: 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 <i>\$srcAddr\$</i> attempted more than <i>\$maxAttempts\$</i> 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 1848: 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 <i>\$srcAddr\$</i> 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 1849: *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 <i>\$srcAddr\$</i> 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 1850: *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 <i>\$srcAddr\$</i> 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 1851: *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 <i>\$srcAddr\$</i> attempted more than <i>\$maxAttempts\$</i> 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 1852: *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 <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | The user access session ended. |
| Recovery | No recovery is required. |

80.17 netconf_user_login

Table 1853: *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 <i>\$srcAddr\$</i> 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 1854: 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 <i>\$srcAddr\$</i> 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 1855: 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 <i>\$srcAddr\$</i> attempted more than <i>\$maxAttempts\$</i> 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 1856: 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 <i>\$srcAddr\$</i> logged out |
| Cause | A user logged out. |
| Effect | The user access session ended. |
| Recovery | No recovery is required. |

80.21 snmp_user_set

Table 1857: 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 <i>\$srcAddr\$</i> > <i>\$vbList\$</i> |
| 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 1858: 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 - <i>\$tmnxVdoNotifysvcId\$</i> , Video interface - <i>\$tmnxVdoNotifyIfName\$</i> , Group address - <i>\$tmnxVdoNotifyGroupAddress\$</i> , Source address - <i>\$tmnxVdoNotifySourceAddress\$</i> , Session Id - <i>\$tmnxVdoNotifyAdSpliceSessionId\$</i> , Abort time - <i>\$tmnxVdoNotifyAdSpliceAbortTime\$</i> , Duration - <i>\$tmnxVdoNotifyAdSpliceDuration\$</i> , Packets - <i>\$tmnxVdoLogAdSplicePackets\$</i> , Octets - <i>\$tmnxVdoLogAdSpliceOctets\$</i> , Bit rate - <i>\$tmnxVdoLogAdSpliceBitRate\$</i> Kbps |
| Cause | This event will be generated when an ad splice is aborted. |
| Effect | N/A |
| Recovery | N/A |

81.2 tmnxVdoClientSessionsLmtCleared

Table 1859: *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 <i>\$tmnxVdoNotifyClientAddress\$</i> |
| Cause | N/A |
| Effect | N/A |
| Recovery | N/A |

81.3 tmnxVdoClientSessionsLmtExceeded

Table 1860: *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 <i>\$tmnxVdoNotifyClientAddress\$</i> |
| Cause | N/A |
| Effect | N/A |

| Property name | Value |
|---------------|-------|
| Recovery | N/A |

81.4 tmnxVdoDuplicateSsrcId

Table 1861: 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 <i>\$tmnxVdoGrpSrcSSRCId\$</i> detected: Service Id - <i>\$svclId\$</i> , Video interface - <i>\$tmnxVdoIfName\$</i> , Group address - <i>\$tmnxVdoGrpSrcGroupAddress\$</i> , Source address - <i>\$tmnxVdoGrpSrcSourceAddress\$</i> |
| 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 1862: 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 - <i>\$tmnxVdoNotifysvcId\$</i> , Video interface - <i>\$tmnxVdoNotifyIfName\$</i> , Group address - <i>\$tmnxVdoNotifyGroupAddress\$</i> , Source address - <i>\$tmnxVdoNotifySourceAddress\$</i> is <i>\$tmnxVdoNotifyAnalyzerState\$</i> |
| 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 1863: 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 - <i>\$tmnxVdoNotifysvcId\$</i> , Video interface - <i>\$tmnxVdoNotifyIfName\$</i> , Group address - <i>\$tmnxVdoNotifyGroupAddress\$</i> , Source address - <i>\$tmnxVdoNotifySourceAddress\$</i> |
| 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 1864: 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 - <i>\$tmnxVdoGrpMdaCurFccBw</i> \$ bandwidth on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1865: 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 - <i>\$tmnxVdoGrpMdaCurFccBw\$</i> bandwidth on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1866: 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 - <i>\$tmnxVdoGrpMdaCurFccRetTotalBw\$</i> bandwidth on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1867: 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 - <i>\$tmnxVdoGrpMdaCurFccRetTotalBw\$</i> bandwidth on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1868: *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 - <i>\$tmnxVdoGrpMdaActFccRetTotalSess\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoMdaFccRetTotSeLmtCleared</i> notification is generated after a <i>tmnxVdoMdaFccRetTotSeLmtExceeded</i> 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 1869: *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 - <i>\$tmnxVdoGrpMdaActFccRetTotalSess\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoMdaFccRetTotSeLmtExceeded</i> 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 1870: *tmnxVdoMdaFccSesLimitCleared* properties

| Property name | Value |
|----------------------------------|---|
| Application name | VIDEO |
| Event ID | 2018 |
| Event name | <i>tmnxVdoMdaFccSesLimitCleared</i> |
| SNMP notification prefix and OID | TIMETRA-VIDEO-MIB. <i>tmnxVdoNotifications.18</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Number of FCC sessions back to the limit - <i>\$tmnxVdoGrpMdaActFccSess\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoMdaFccSesLimitCleared</i> notification is generated after a <i>tmnxVdoMdaFccSesLimitExceeded</i> 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 1871: 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 - <i>\$tmnxVdoGrpMdaActFccSess\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1872: 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 - <i>\$tmnxVdoGrpMdaCurAbsRetBw</i> \$ bandwidth on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoMdaRetBwLimitCleared</i> notification is generated after a <i>tmnxVdoMdaRetBwLimitExceeded</i> 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 1873: *tmnxVdoMdaRetBwLimitExceeded* properties

| Property name | Value |
|----------------------------------|---|
| Application name | VIDEO |
| Event ID | 2013 |
| Event name | <i>tmnxVdoMdaRetBwLimitExceeded</i> |
| SNMP notification prefix and OID | TIMETRA-VIDEO-MIB. <i>tmnxVdoNotifications.13</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Threshold for RET bandwidth exceeded - <i>\$tmnxVdoGrpMdaCurAbsRetBw\$</i> bandwidth on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoMdaRetBwLimitExceeded</i> 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 1874: 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 - <i>\$tmnxVdoGrpMdaActRet Sess\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlot Num\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1875: 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 - <i>\$tmnxVdoGrpMdaActRetSess\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoMdaRetSesLimitExceeded</i> 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 1876: *tmnxVdoMdaSessionsLimitCleared* properties

| Property name | Value |
|----------------------------------|--|
| Application name | VIDEO |
| Event ID | 2004 |
| Event name | <i>tmnxVdoMdaSessionsLimitCleared</i> |
| SNMP notification prefix and OID | TIMETRA-VIDEO-MIB. <i>tmnxVdoNotifications.4</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Number of RTCP sessions back to the limit - <i>\$tmnxVdoGrpMdaActiveRtcpSessions\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1877: 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 - <i>\$tmnxVdoGrpMdaActiveRtcpSessions\$</i> sessions active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1878: 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 - <i>\$tmnxVdoGrpMdaChannels\$</i> channels active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1879: *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 - <i>\$tmnxVdoGrpMdaChannels\$</i> channels active on MDA <i>\$tmnxChassisIndex\$/\$tmnxCardSlotNum\$/\$tmnxMDASlotNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1880: *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 - <i>\$tmnxVdoGrpVappCurFccBw\$</i> bandwidth on VAPP <i>\$tmnxVdoGrpEsaNum\$/\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A <i>tmnxVdoVappFccBwLimitCleared</i> notification is generated after a <i>tmnxVdoVappFccBwLimitExceeded</i> 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 1881: *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 - <i>\$tmnxVdoGrpVappCurFccBw</i> \$ bandwidth on VAPP <i>\$tmnxVdoGrpEsaNum</i> /\$ <i>\$tmnxVdoGrpEsaVappNum</i> \$, video group - <i>\$tmnxVdoGrpId</i> \$ |
| Cause | A <i>tmnxVdoVappFccBwLimitExceeded</i> 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 1882: *tmnxVdoVappFccRetTotBwLmtCleared* properties

| Property name | Value |
|----------------------------------|---|
| Application name | VIDEO |
| Event ID | 2032 |
| Event name | <i>tmnxVdoVappFccRetTotBwLmtCleared</i> |
| SNMP notification prefix and OID | TIMETRA-VIDEO-MIB. <i>tmnxVdoNotifications.32</i> |
| Default severity | warning |
| Source stream | main |
| Message format string | Total FCC and RET bandwidth back to the limit - <i>\$tmnxVdoGrpVappCurFccRetTotalBw</i> \$ bandwidth on VAPP <i>\$tmnxVdoGrpEsaNum</i> /\$ <i>\$tmnxVdoGrpEsaVappNum</i> \$, video group - <i>\$tmnxVdoGrpId</i> \$ |
| Cause | A <i>tmnxVdoVappFccRetTotBwLmtCleared</i> notification is generated after a <i>tmnxVdoVappFccRetTotBwLmtExceeded</i> 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 tmnxVdoVappFccRetTotBwLmtExceeded

Table 1883: tmnxVdoVappFccRetTotBwLmtExceeded properties

| Property name | Value |
|----------------------------------|--|
| Application name | VIDEO |
| Event ID | 2031 |
| Event name | tmnxVdoVappFccRetTotBwLmtExceeded |
| 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 - <i>\$tmnxVdoGrpVappCurFccRetTotalBw\$</i> bandwidth on VAPP <i>\$tmnxVdoGrpEsaNum\$/\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| Cause | A tmnxVdoVappFccRetTotBwLmtExceeded 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 1884: 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 - $\$tmnxVdoGrpld\$$ |
| Cause | A $tmnxVdoVappFccRetTotSeLmtCleared$ notification is generated after a $tmnxVdoVappFccRetTotSeLmtExceeded$ 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 $tmnxVdoVappFccRetTotSeLmtExceeded$

Table 1885: $tmnxVdoVappFccRetTotSeLmtExceeded$ properties

| Property name | Value |
|----------------------------------|---|
| Application name | VIDEO |
| Event ID | 2037 |
| Event name | $tmnxVdoVappFccRetTotSeLmtExceeded$ |
| 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 - $\$tmnxVdoGrpld\$$ |
| Cause | A $tmnxVdoVappFccRetTotSeLmtExceeded$ 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 1886: 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 - <i>\$tmnxVdoGrpVappActFcc Sess\$</i> sessions active on VAPP <i>\$tmnxVdoGrpEsaNum\$</i> / <i>\$tmnxVdoGrp EsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1887: 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 - <i>\$tmnxVdoGrpVappActFccSess\$</i> sessions active on VAPP <i>\$tmnxVdoGrpEsaNum\$/\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1888: 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 - <i>\$tmnxVdoGrpVappCurAbsRetBw\$</i> bandwidth on VAPP <i>\$tmnxVdoGrpEsaNum\$/\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1889: 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 1890: 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 - <i>\$tmnxVdoGrpVappActRetSess\$</i> sessions active on VAPP <i>\$tmnxVdoGrpEsaNum\$</i> / <i>\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1891: 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 - <i>\$tmnxVdoGrpVappActRetSess\$</i> sessions active on VAPP <i>\$tmnxVdoGrpEsaNum\$</i> / <i>\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1892: 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 - <i>\$tmnxVdoGrpVappActiveRtcpSessions\$</i> sessions active on VAPP <i>\$tmnxVdoGrpEsaNum\$</i> / <i>\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1893: 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 - <i>\$tmnxVdoGrpVappActiveRtcpSessions\$</i> sessions active on VAPP <i>\$tmnxVdoGrpEsaNum\$</i> / <i>\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpld\$</i> |
| 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 1894: 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 - <i>\$tmnxVdoGrpVappChannels\$</i> channels active on VAPP <i>\$tmnxVdoGrpEsaNum\$</i> / <i>\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpld\$</i> |
| 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 1895: 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 - <i>\$tmnxVdoGrpVapp Channels\$</i> channels active on VAPP <i>\$tmnxVdoGrpEsaNum\$/\$tmnxVdoGrpEsaVappNum\$</i> , video group - <i>\$tmnxVdoGrpId\$</i> |
| 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 1896: 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 <i>\$vrrpOperVrld\$</i> on interface <i>\$ifIndex\$</i> changed state to backup - current master is <i>\$vrrpOperMasterIpAddr\$</i> |
| Cause | The sending agent has transitioned to 'Backup' state. |
| Effect | N/A |
| Recovery | N/A |

82.2 tmnxVrrpBfdIntfSessStateChgd

Table 1897: 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 <i>\$tmnxVrrpNotifBfdIntfSvcId\$</i> interface <i>\$tmnxVrrpNotifBfdIntfName\$</i> to peer <i>\$tmnxVrrpNotifBfdIntfDestIp\$</i> changed state to <i>\$tmnxVrrpNotifBfdIntfSessState\$</i> . |
| Cause | The operational state of a BFD session of the VRRP instance changed. |
| Effect | N/A |
| Recovery | N/A |

82.3 tmnxVrrpIPListMismatch

Table 1898: *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 <i>\$tmnxVrrpRouterMasterPrimaryAddr\$</i> did not match address list configured for VRRP instance <i>\$vrrpOperVrld\$</i> on interface <i>\$ifIndex\$</i> |
| 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 1899: 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 <i>\$vrrpOperVrld\$</i> on interface <i>\$ifIndex\$</i> for advertisements from <i>\$tmnxVrrpRouterMasterPrimaryAddr\$</i> |
| 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 1900: 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 | <i>\$tmnxVrrpRouterMasterPrimaryAddr\$</i> is advertising itself as an owner for VRRP instance <i>\$vrrpOperVrld\$</i> which conflicts with owner instance on interface <i>\$ifIndex\$</i> |
| 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 1901: *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 <i>\$vrrpOperVrld\$</i> on interface <i>\$ifIndex\$</i> . 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 1902: 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 \$vrrpOperVrld\$ 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 1903: 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 <i>\$vrrpOperationsVrld\$</i> on interface <i>\$ifIndex\$</i> changed state to backup - current master is <i>\$vrrpOperationsMasterIpAddr\$</i> |
| Cause | The sending agent has transitioned to 'Backup' state. |
| Effect | N/A |
| Recovery | N/A |

82.9 tVrrpIPListMismatch

Table 1904: 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 <i>\$tVrrpRtrMasterPrimaryAddr\$</i> did not match address list configured for VRRP instance <i>\$vrrpOperationsVrld\$</i> on interface <i>\$ifIndex\$</i> |
| 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 1905: 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 <i>\$vrrpOperationsVrld\$</i> on interface <i>\$ifIndex\$</i> for advertisements from <i>\$tVrrpRtrMasterPrimaryAddr\$</i> |
| 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 1906: 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 | <i>\$tVrrpRtrMasterPrimaryAddr\$</i> is advertising itself as an owner for VRRP instance <i>\$vrrpOperationsVrld\$</i> which conflicts with owner instance on interface <i>\$ifIndex\$</i> |
| 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 1907: 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 <i>\$vrrpOperationsVrld\$</i> on interface <i>\$ifIndex\$</i> . 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 1908: 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 1909: 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 <i>\$vrrpPacketSrc\$</i> because <i>\$vrrpPacketDiscardReason\$</i> |
| 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 1910: 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 <i>\$ifIndex\$</i> of VR <i>\$vrrpOperationsVrId\$</i> 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 1911: 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 <i>\$vrrpOperationsVrld\$</i> on interface <i>\$ifIndex\$</i> 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 1912: 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 <i>\$vrrpOperationsVrld\$</i> on interface <i>\$ifIndex\$</i> (primary address <i>\$vrrpOperationsMasterIpAddr\$</i>) changed state to master due to <i>\$vrrpNewMasterReason\$</i> |
| Cause | The sending agent has transitioned to 'Master' state. |
| Effect | N/A |
| Recovery | N/A |

82.18 vrrpPacketDiscarded

Table 1913: 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 <i>\$vrrpPacketSrc\$</i> because <i>\$vrrpPacketDiscardReason\$</i> |
| 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 1914: 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 <i>\$vrrpTrapPacket Src\$</i> because <i>\$vrrpTrapAuthErrorType\$</i> |
| 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 1915: 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 <i>\$vrrpOperVrld\$</i> on interface <i>\$ifIndex\$</i> (primary address <i>\$vrrpOperMasterIpAddr\$</i>) changed state to master |
| Cause | The sending agent has transitioned to 'Master' state. |
| Effect | N/A |
| Recovery | N/A |

82.21 vrrpTrapProtoError

Table 1916: 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 <i>\$vrrpTrapProtoErrReason\$</i> |
| Cause | The sending agent encountered a protocol error. |
| Effect | N/A |
| Recovery | N/A |

83 VRTR

83.1 tipNbrAllocFailed

Table 1917: 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 <i>\$neighbor\$</i> on itf <i>\$interface\$</i> |
| 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 1918: 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 <i>\$vRtrIfName\$</i> : Number of ARP entries learned has exceeded the configured maximum (<i>\$vRtrIfArpLimit\$</i>) |
| Cause | A <i>tmnxVRtrArpLmt</i> 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 <i>vRtrIfArpLimit</i> . No new entries are learned until an entry expires. |
| Recovery | Increase the arp-limit. |

83.3 *tmnxVRtrArpThresholdExceeded*

Table 1919: *tmnxVRtrArpThresholdExceeded* properties

| Property name | Value |
|----------------------------------|---|
| Application name | VRTR |
| Event ID | 2078 |
| Event name | <i>tmnxVRtrArpThresholdExceeded</i> |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB. <i>tmnxVRtrNotifications.78</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Interface <i>\$vRtrIfName\$</i> : Number of ARP entries learned has exceeded the <i>\$vRtrIfArpThreshold\$</i> percentage of the configured maximum (<i>\$vRtrIfArpLimit\$</i>) |
| Cause | A <i>tmnxVRtrArpThresholdExceeded</i> notification is generated when the number of IPv4 ARP entries learned on an IP interface has exceeded <i>vRtrIfArpThreshold</i> percent of the configured maximum as specified by <i>vRtrIfArpLimit</i> . |
| 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 <i>vRtrIfArpLimit</i> . 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 1920: 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 <i>\$vRtrIfBfdSessExtLclDisc\$</i> on node <i>\$subject\$</i> 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 1921: 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 <i>\$vRtrIfBfdSessExtLclDisc\$</i> on node <i>\$subject\$</i> 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 1922: 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 <i>\$vRtrBfdAllocateGroup\$</i> BFD sessions on <i>\$vRtrSlotOrCpmFlag\$ \$vRtrBfdSlotNumber\$</i> has exceeded the limit of <i>\$vRtrNumberOfBfdSessionsOnSlot\$</i> sessions, constrained by <i>\$vRtrBfdMaxSessionReason\$</i> . |

| Property name | Value |
|---------------|--|
| Cause | The tmnxVRtrBfdMaxSessionOnSlot notification is generated for several reasons, indicated by vRtrBfdMaxSessionReason. When 'maxSessionsPerSlot' the maximum number of BFD sessions indicated by vRtrNumberOfBfdSessionsOnSlot has been reached, when 'maxTxPacketRate' or 'maxRxPacketRate' then the maximum transmit or receive packet rate limit is exceeded, indicated by vRtrAllocatedBfdTxPacketRate or vRtrAllocatedBfdRxPacketRate. The location where the limit has been reached is indicated by vRtrSlotOrCpmFlag. vRtrBfdSlotNumber 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 1923: 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 <i>\$vRtrIfBfdSessExtLclDisc\$</i> on interface <i>\$vRtrIfIndex\$</i> (local <i>\$vRtrIfBfdSessExtLclAddr\$</i> , remote <i>\$vRtrIfBfdSessExtRemAddr\$</i>) will go down if peer packets do not arrive on slot <i>\$vRtrBfdSlotNumber\$</i> , FP <i>\$vRtrNotifyFpNum\$</i> |
| 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 1924: 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 <i>\$tmnxPortType\$</i> ports. No sessions will come up on port <i>\$tmnxPortNotifyPortId\$</i> . |
| Cause | BFD is not supported on the port specified. |
| Effect | N/A |
| Recovery | N/A |

83.9 tmnxVRtrBfdSessExtDeleted

Table 1925: 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 <i>\$subject\$</i> 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 1926: 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 <i>\$vRtrIfBfdSessExtLclDisc\$</i> BFD session on node <i>\$subject\$</i> is down due to <i>\$vRtrIfBfdSessExtOperFlags\$</i> |
| 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 1927: 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(<i>\$vRtrIfBfdSessChangedProtocol\$</i>) using BFD session on node <i>\$subject\$</i> has been <i>\$vRtrIfBfdSessProtoChngdState\$</i> . |
| 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 1928: 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 <i>\$vRtrIfBfdSessExtLc/Disc\$</i> BFD session on node <i>\$subject\$</i> is up |
| Cause | The <i>tmnxVRtrBfdSessExtUp</i> 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 1929: *tmnxVRtrDhcp6ClientStatusChanged* properties

| Property name | Value |
|----------------------------------|--|
| Application name | VRTR |
| Event ID | 2087 |
| Event name | <i>tmnxVRtrDhcp6ClientStatusChanged</i> |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB. <i>tmnxVRtrNotifications.87</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Interface <i>\$vRtrIfIndex\$</i> : DHCPv6 client status changed to <i>\$vRtrIfDhcp6CISStateStatus\$</i> - <i>\$vRtrIfDhcp6CISStateDescription\$</i> |
| Cause | The <i>tmnxVRtrDhcp6ClientStatusChanged</i> notification is sent when the value of the object <i>vRtrIfDhcp6CISStateStatus</i> changes. |
| Effect | While the value of the object <i>vRtrIfDhcp6CISStateDescription</i> 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 <i>vRtrIfDhcp6CISStateDescription</i> . |

83.14 *tmnxVRtrDhcpClientStatusChanged*

Table 1930: *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 <i>\$vRtrIfIndex\$</i> : DHCP client status changed to <i>\$vRtrIfDhcpCISStateStatus\$</i> - <i>\$vRtrIfDhcpCISStateDescription\$</i> |
| Cause | The <i>tmnxVRtrDhcpClientStatusChanged</i> notification is sent when the value of the object <i>vRtrIfDhcpCISStateStatus</i> changes. |
| Effect | While the value of the object <i>vRtrIfDhcpCISStateDescription</i> 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 <i>vRtrIfDhcpCISStateDescription</i> . |

83.15 tmnxVRtrDnsFault

Table 1931: *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 <i>\$vRtrNotifNetAddr\$</i> <i>\$vRtrNotifTruthValue\$</i> - <i>\$vRtrFailureDescription\$</i> |

| 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, vRtrNotiflNetAddrType, and vRtrNotiflNetAddr. 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 1932: 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 1933: *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 1934: *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 <i>\$vRtrGrtMaxExportRoutes\$</i> , 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 tmnxVRtrGrRoutesExpLimitDropped

Table 1935: tmnxVRtrGrRoutesExpLimitDropped properties

| Property name | Value |
|----------------------------------|---|
| Application name | VRTR |
| Event ID | 2027 |
| Event name | tmnxVRtrGrRoutesExpLimitDropped |
| 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 \$vRtrGrMaxExportRoutes\$ |
| Cause | Number of exported routes into GRT has dropped below the configured export limit. |
| Effect | N/A |
| Recovery | N/A |

83.20 tmnxVRtrGrV6ExportLimitReached

Table 1936: tmnxVRtrGrV6ExportLimitReached properties

| Property name | Value |
|----------------------------------|---|
| Application name | VRTR |
| Event ID | 2032 |
| Event name | tmnxVRtrGrV6ExportLimitReached |
| 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 <i>\$vRtrGrMaxIpv6ExportRoutes \$</i> , 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 tmnxVRtrGrV6RoutesExpLimDropped

Table 1937: *tmnxVRtrGrV6RoutesExpLimDropped* properties

| Property name | Value |
|----------------------------------|---|
| Application name | VRTR |
| Event ID | 2033 |
| Event name | tmnxVRtrGrV6RoutesExpLimDropped |
| 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 <i>\$vRtrGrMaxIpv6ExportRoutes\$</i> |
| 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 1938: *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 <i>\$subject\$</i> has cleared the high-level threshold: <i>\$vRtrHighRouteThreshold\$</i> - the routing table contains <i>\$vRtrStatCurrNumRoutes\$</i> routes |
| Cause | The number of routes has dropped below the high-level threshold. |
| Effect | N/A |
| Recovery | N/A |

83.23 tmnxVRtrHighRouteTCA

Table 1939: *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 <i>\$subject\$</i> has exceeded the high-level threshold: <i>\$vRtrHighRouteThreshold\$</i> - the routing table contains <i>\$vRtrStatCurrNumRoutes\$</i> 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 1940: 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: <i>\$vRtrServiceId\$</i> for IP interface: <i>\$vRtrIfName\$</i> is <i>\$vRtrNotifIgnorePortState\$</i> |
| 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 1941: 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 <i>\$vRtrIfName\$</i> with timer value <i>\$vRtrIfLdpSyncTimer\$</i> |
| Cause | LDP Sync timer started for the interface. |
| Effect | N/A |
| Recovery | N/A |

83.26 tmnxVRtrIfLdpSyncTimerStop

Table 1942: 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 <i>\$vRtrIfName\$</i> with timer value <i>\$vRtrIfLdpSyncTimer\$</i> |
| Cause | LDP Sync timer stops for the interface. |
| Effect | N/A |
| Recovery | N/A |

83.27 tmnxVRtrInetAddressAttachFailed

Table 1943: 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 1944: 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 <i>\$subject\$</i> has cleared the high-level threshold: <i>\$vRtrIPv6HighRouteThreshold\$</i> - the routing table contains <i>\$vRtrV6StatCurrNumRoutes\$</i> 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 1945: 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 <i>\$subject\$</i> has exceeded the high-level threshold: <i>\$vRtrIPv6HighRouteThreshold\$</i> - the routing table contains <i>\$vRtrV6StatCurrNumRoutes\$</i> 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 1946: *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 <i>\$subject\$</i> has exceeded the mid-level threshold: <i>\$vRtrIPv6MidRouteThreshold\$</i> - the routing table contains <i>\$vRtrV6StatCurrNumRoutes\$</i> 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 1947: *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 <i>\$vRtrIfName\$</i> : Number of neighbor entries learned has exceeded the configured maximum (<i>\$vRtrIpv6NbrLimit\$</i>) |

| 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 vRtrIflpv6NbrLimit. No new entries are learned until an entry expires. |
| Recovery | Increase the neighbor limit. |

83.32 tmnxVRtrIpv6NbrThresholdExceeded

Table 1948: 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 <i>\$vRtrIflName\$</i> : Number of neighbor entries learned has exceeded the <i>\$vRtrIflpv6NbrThreshold\$</i> percentage of the configured maximum (<i>\$vRtrIflpv6NbrLimit\$</i>) |
| Cause | A tmnxVRtrIpv6NbrThresholdExceeded notification is generated when the number of IPv6 neighbor entries learned on an IP interface has exceeded vRtrIflpv6NbrThreshold percent of the configured maximum as specified by vRtrIflpv6NbrLimit. |
| 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 vRtrIflpv6NbrLimit. 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 1949: 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 <i>\$vRtrLeakExportLimit\$</i> |
| 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 1950: 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 <i>\$vRtrLeakExportLimit\$</i> , additional routes will not be exported into VPRN |
| Cause | The <i>tmnxVRtrLeakExportLimitReached</i> 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 1951: *tmnxVRtrMacAcctLimitCleared* properties

| Property name | Value |
|----------------------------------|--|
| Application name | VRTR |
| Event ID | 2068 |
| Event name | <i>tmnxVRtrMacAcctLimitCleared</i> |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB. <i>tmnxVRtrNotifications.68</i> |
| Default severity | minor |
| Source stream | main |
| Message format string | Mac Accounting Indices are available for RtrId <i>\$vRtrID\$</i> Interface <i>\$vRtrIfName\$</i> |
| Cause | The <i>tmnxVRtrMacAcctLimitCleared</i> notification is generated when one or more MAC entries are deleted following the generation of a <i>tmnxVRtrMacAcctLimitReached</i> 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 1952: *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 1953: *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 <i>\$vRtrManagedRouteInetAddr\$</i> / <i>\$vRtrManagedRoutePrefixLen\$</i> in router <i>\$subject\$</i> : <i>\$vRtrFailureDescription\$</i> |
| Cause | A managed route could not be installed. |
| Effect | N/A |
| Recovery | N/A |

83.38 tmnxVRtrMaxArpEntriesCleared

Table 1954: 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 <i>\$subject\$</i> has cleared the maximum ARP entries threshold: <i>\$vRtrMaxARPEnties\$</i> - its ARP table contains <i>\$vRtrStatActiveARPEnties\$</i> active entries and <i>\$vRtrStatTotalARPEnties\$</i> 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 1955: *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 <i>\$subject\$</i> has caused the maximum ARP entries threshold for the system to be crossed: <i>\$vRtrMaxARPEntries\$</i> - its ARP table contains <i>\$vRtrStatActiveARPEntries\$</i> active entries and <i>\$vRtrStatTotalARPEntries\$</i> total entries |
| Cause | The maximum ARP entries threshold for all Routers has been crossed. |
| Effect | N/A |
| Recovery | N/A |

83.40 tmnxVRtrMaxRoutes

Table 1956: *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 <i>\$subject\$</i> has exceeded the max <i>\$vRtrMaxRoutesType\$</i> routes threshold: <i>\$vRtrMaxNumRoutes\$</i> - the VRF contains <i>\$vRtrStatCurrNumRoutes\$</i> 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 1957: 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 <i>\$subject\$</i> has cleared the high-level threshold for multicast routes: <i>\$vRtrMaxMcastNumRoutes\$</i> - the multicast routing table contains <i>\$vRtrMulticastRoutes\$</i> 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 1958: 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 <i>\$subject\$</i> has exceeded the max multicast routes threshold: <i>\$vRtrMaxMcastNumRoutes\$</i> - the multicast routing table contains <i>\$vRtrMulticastRoutes\$</i> routes |
| Cause | The max routes threshold for number of multicast routes has been crossed. |
| Effect | N/A |
| Recovery | N/A |

83.43 tmnxVRtrMcastMidRouteTCA

Table 1959: 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 <i>\$subject\$</i> has exceeded the mid-level threshold for multicast routes: <i>\$vRtrMcastMidRouteThreshold\$</i> - the multicast routing table contains <i>\$vRtrMulticastRoutes\$</i> 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 1960: 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 <i>\$subject\$</i> has exceeded the mid-level threshold: <i>\$vRtrMidRouteThreshold\$</i> - the routing table contains <i>\$vRtrStatCurrNumRoutes\$</i> routes |
| Cause | The mid-level threshold for number of routes has been crossed. |
| Effect | N/A |
| Recovery | N/A |

83.45 tmnxVRtrNeDiscovered

Table 1961: 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 | <p>Possible messages:</p> <ul style="list-style-type: none"> New NE discovered: RtrId \$vRtrID\$, NEID 0x\$tmnxVRtrNeInfoNeid\$, NEIP (ipv4 \$tmnxVRtrNeInfoNeipV4\$/ \$tmnxVRtrNeInfoNeipV4PrefixLen\$, ipv6 N.A.), system-mac \$tmnxVRtrNeInfoSystemMac\$, vendor-id \$tmnxVRtrNeInfoVendorId\$, platform-type \$tmnxVRtrNeInfoPlatformType\$ New NE discovered: RtrId \$vRtrID\$, NEID 0x\$tmnxVRtrNeInfoNeid\$, NEIP (ipv4 \$tmnxVRtrNeInfoNeipV4\$/ \$tmnxVRtrNeInfoNeipV4PrefixLen\$, ipv6 \$tmnxVRtrNeInfoNeipV6\$/ \$tmnxVRtrNeInfoNeipV6PrefixLen\$), system-mac \$tmnxVRtrNeInfoSystemMac\$, vendor-id \$tmnxVRtrNeInfoVendorId\$, platform-type \$tmnxVRtrNeInfoPlatformType\$ |
| 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 1962: 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 | <p>Possible messages:</p> <ul style="list-style-type: none"> NE modified: RtrId \$vRtrID\$, NEID 0x\$tmnxVRtrNeInfoNeid\$, NEIP (ipv4 \$tmnxVRtrNeInfoNeipV4\$/ \$tmnxVRtrNeInfoNeipV4PrefixLen\$, ipv6 N.A.), system-mac \$tmnxVRtrNeInfoSystemMac\$, vendor- |

| Property name | Value |
|---------------|--|
| | id <i>\$tmnxVRtrNeInfoVendorId\$</i> , platform-type <i>\$tmnxVRtrNeInfoPlatformType\$</i> <ul style="list-style-type: none"> NE modified: RtrId <i>\$vRtrID\$</i>, NEID 0x<i>\$tmnxVRtrNeInfoNeid\$</i>, NEIP (ipv4 <i>\$tmnxVRtrNeInfoNeipV4\$/\$tmnxVRtrNeInfoNeipV4PrefixLen\$</i>, ipv6 <i>\$tmnxVRtrNeInfoNeipV6\$/\$tmnxVRtrNeInfoNeipV6PrefixLen\$</i>), system-mac <i>\$tmnxVRtrNeInfoSystemMac\$</i>, vendor-id <i>\$tmnxVRtrNeInfoVendorId\$</i>, platform-type <i>\$tmnxVRtrNeInfoPlatformType\$</i> |
| Cause | The tmnxVRtrNeModified notification is sent when a Network Element is modified. |
| Effect | No effect. |
| Recovery | No recovery is necessary. |

83.47 tmnxVRtrNeRemoved

Table 1963: 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: <ul style="list-style-type: none"> NE removed: RtrId <i>\$vRtrID\$</i>, NEID 0x<i>\$tmnxVRtrNeInfoNeid\$</i>, NEIP (ipv4 <i>\$tmnxVRtrNeInfoNeipV4\$/\$tmnxVRtrNeInfoNeipV4PrefixLen\$</i>, ipv6 N.A.), system-mac <i>\$tmnxVRtrNeInfoSystemMac\$</i>, vendor-id <i>\$tmnxVRtrNeInfoVendorId\$</i>, platform-type <i>\$tmnxVRtrNeInfoPlatformType\$</i> NE removed: RtrId <i>\$vRtrID\$</i>, NEID 0x<i>\$tmnxVRtrNeInfoNeid\$</i>, NEIP (ipv4 <i>\$tmnxVRtrNeInfoNeipV4\$/\$tmnxVRtrNeInfoNeipV4PrefixLen\$</i>, ipv6 <i>\$tmnxVRtrNeInfoNeipV6\$/\$tmnxVRtrNeInfoNeipV6PrefixLen\$</i>), system-mac <i>\$tmnxVRtrNeInfoSystemMac\$</i>, vendor-id <i>\$tmnxVRtrNeInfoVendorId\$</i>, platform-type <i>\$tmnxVRtrNeInfoPlatformType\$</i> |

| 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 1964: 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 \$vRtrIfBfdSessExtLcIDisc\$ 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 1965: *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 | <i>\$vRtrIfBfdSessExtLinkType\$</i> BFD session with Local Discriminator <i>\$vRtrIfBfdSessExtLcIDisc\$</i> on <i>\$subject\$</i> has been deleted |
| Cause | The <i>tmnxVRtrNgBfdSessDeleted</i> 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 1966: *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 | <i>\$vRtrIfBfdSessExtLinkType\$</i> BFD session with Local Discriminator <i>\$vRtrIfBfdSessExtLcIDisc\$</i> on <i>\$subject\$</i> is down due to <i>\$vRtrIfBfdSessExtOperFlags\$</i> |

| 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 1967: 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 (<i>\$vRtrIfBfdSessChangedProtocol\$</i>) using <i>\$vRtrIfBfdSess ExtLinkType\$</i> BFD session on <i>\$subject\$</i> has been <i>\$vRtrIfBfdSessProto ChngdState\$</i> . |
| 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 1968: *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 | <i>\$vRtrIfBfdSessExtLinkType\$</i> BFD session with Local Discriminator <i>\$vRtrIfBfdSessExtLcDisc\$</i> on <i>\$subject\$</i> 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 1969: *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 <i>\$tmnxVRtrMaxNHRvplsARPEntries\$</i> |

| 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 tmnxVRtrMaxNHRvplsARPEnties. |
| 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 1970: 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 \$tmnxVRtrMaxNHRvplsARPEnties\$ |
| Cause | The tmnxVRtrNHRvplsARPHighUsage notification is generated when Nexthop RVPLS ARP entries reaches 95% of its limit as indicated by the value of tmnxVRtrMaxNHRvplsARPEnties. |
| 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 1971: *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 <i>\$tmnxVRtrMaxNHRvplsARPEntries\$</i> |
| 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 1972: *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 <i>\$vRtrID\$</i> PDN interface <i>\$vRtrIfName\$</i> PDN IP address <i>\$vRtrNotifInetAddr\$</i> mismatch - <i>\$vRtrFailureDescription\$</i> |

| 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 1973: 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 1974: 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 : <i>\$vRtrSingleSfmOverloadState\$</i> |
| 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 1975: 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 <i>\$vRtrID\$</i> , the static route CPE check for <i>\$vRtrInetStatRteCpeNotifyAddr\$</i> has transitioned to <i>\$vRtrInetStaticRouteCpeStatus\$</i> . |
| Cause | A CPE associated with a static route, as specified by the <i>vRtrInetStaticRouteCpeAddr</i> object, became reachable or unreachable. |
| Effect | N/A |
| Recovery | N/A |

83.60 tmnxVRtrStaticRouteStatusChanged

Table 1976: *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 <i>\$vRtrInetStaticRouteStaticType\$</i> is <i>\$vRtrInetStaticRouteStatus\$</i> . The static route next hop and next hop interface is <i>\$vRtrInetStaticRouteNextHop\$</i> and <i>\$vRtrInetStaticRouteNextHopIf\$</i> 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 1977: 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 \$vRtrAutoCfgRaRtStatus\$ |
| 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 vRtrBgplInstanceError

Table 1978: vRtrBgplInstanceError properties

| Property name | Value |
|----------------------------------|--|
| Application name | VRTR |
| Event ID | 2101 |
| Event name | vRtrBgplInstanceError |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.101 |
| Default severity | minor |

| Property name | Value |
|-----------------------|---|
| Source stream | main |
| Message format string | Virtual router <i>\$vRtrID\$</i> BGP type <i>\$vRtrNotifyBgpInstType\$</i> and instance <i>\$vRtrNotifyBgpInstance\$</i> had error: <i>\$vRtrFailureDescription\$</i> |
| 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 vRtrIfDhcp6CISateDnsChanged

Table 1979: vRtrIfDhcp6CISateDnsChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | VRTR |
| Event ID | 2094 |
| Event name | vRtrIfDhcp6CISateDnsChanged |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.94 |
| Default severity | minor |
| Source stream | main |
| Message format string | Interface <i>\$vRtrIfIndex\$</i> : DHCP6 client DNS addresses changed to DNS1= <i>\$vRtrIfDhcp6CISateDnsPriAddr\$</i> DNS2= <i>\$vRtrIfDhcp6CISateDnsSecAddr\$</i> DNS3= <i>\$vRtrIfDhcp6CISateDnsTerAddr\$</i> |
| Cause | The vRtrIfDhcp6CISateDnsChanged notification is sent when the value of any of the DNS addresses of the DHCP6 client changes. |
| Effect | [RECOVERY] |
| Recovery | N/A |

83.64 vRtrIfDhcpCIRtStatusChanged

Table 1980: vRtrIfDhcpCIRtStatusChanged properties

| Property name | Value |
|----------------------------------|--|
| Application name | VRTR |
| Event ID | 2091 |
| Event name | vRtrIfDhcpCIRtStatusChanged |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.91 |
| Default severity | minor |
| Source stream | main |
| Message format string | Interface \$vRtrIfIndex\$: DHCP client route \$vRtrIfDhcpCIRtAddr\$/\$vRtrIfDhcpCIRtPrefixLen\$ next-hop \$vRtrIfDhcpCIRtNhAddr\$ status changed to \$vRtrIfDhcpCIRtStatus\$ |
| Cause | The vRtrIfDhcpCIRtStatusChanged notification is sent when the value of the object vRtrIfDhcpCIRtStatus changes; that includes when a row in the vRtrIfDhcpCIRtTable 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 vRtrIfDhcpCIStateDnsChanged

Table 1981: vRtrIfDhcpCIStateDnsChanged properties

| Property name | Value |
|----------------------------------|---|
| Application name | VRTR |
| Event ID | 2092 |
| Event name | vRtrIfDhcpCIStateDnsChanged |
| SNMP notification prefix and OID | TIMETRA-VRTR-MIB.tmnxVRtrNotifications.92 |
| Default severity | minor |
| Source stream | main |

| Property name | Value |
|-----------------------|---|
| Message format string | Interface <i>\$vRtrIfIndex\$</i> : DHCP client DNS addresses changed to DNS1= <i>\$vRtrIfDhcpCISateDnsPriAddr\$</i> DNS2= <i>\$vRtrIfDhcpCISateDnsSecAddr\$</i> DNS3= <i>\$vRtrIfDhcpCISateDnsTerAddr\$</i> |
| Cause | The vRtrIfDhcpCISateDnsChanged 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 1982: 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 <i>\$vRtrIfIndex\$</i> : 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 1983: 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 1984: 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 1985: 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 <i>\$tmnxWlanGwNotifyBdBridgeId\$</i> 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 1986: 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 <i>\$tmnxWlanGwNotifyBdBridgeId\$</i> 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 1987: 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 <i>\$tmnxCardSlotNum\$/\$tmnxWlanGwNotifyMdaSlotNum\$</i> in WLAN Gateway group <i>\$tmnxWlanGwGrpId\$ - \$tmnxWlanGwNotifyDescription\$</i> . |
| 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 1988: 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 <i>\$tmnxWlanGwNotifyEntity\$</i> usage high water status changed to <i>\$tmnxWlanGwNotifyTrue\$</i> on ISA group <i>\$tmnxWlanGwNotifyIsaGrpId\$</i> member <i>\$tmnxWlanGwNotifyIsaMemberId\$</i> on <i>\$tmnxWlanGwNotifyChassisIndex\$/\$tmnxWlanGwNotifyCardSlotNum\$/\$tmnxWlanGwNotifyMdaSlotNum\$</i> . (EsaNum <i>\$tmnxWlanGwNotifyEsaNum\$</i> , EsaVappNum <i>\$tmnxWlanGwNotifyEsaVappNum\$</i>) |
| 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 1989: 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 <i>\$tmnxWlanGwGrpId\$</i> changed to <i>\$tmnxWlanGwGrpOperState\$</i> . |
| Cause | The tmnxWlanGwGrpOperStateChanged notification is sent when the value of the object tmnxWlanGwGrpOperState changes. |
| Effect | N/A |
| Recovery | N/A |

84.6 tmnxWlanGwGtpMessageDropped

Table 1990: 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 <i>\$tmnxWlanGwNotifyGtpMsgDirection\$</i> message (type <i>\$tmnxWlanGwNotifyGtpMsgType\$</i> version <i>\$tmnxWlanGwMgwControl\$</i> IMSI <i>\$tmnxWlanGwNotifyImsi\$</i> TEID <i>\$tmnxWlanGwNotifyTeid\$</i>) dropped from/to Mobile Gateway <i>\$tmnxWlanGwMgwRemoteAddr\$</i> port <i>\$tmnxWlanGwMgwRemotePort\$</i> in router <i>\$vRtrID\$</i> - <i>\$tmnxWlanGwNotifyDescription\$</i> |
| 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 tmnxWlanGwlomActive

Table 1991: tmnxWlanGwlomActive properties

| Property name | Value |
|----------------------------------|---|
| Application name | WLAN_GW |
| Event ID | 2005 |
| Event name | tmnxWlanGwlomActive |
| SNMP notification prefix and OID | TIMETRA-WLAN-GW-MIB.tmnxWlanGwNotifications.5 |
| Default severity | minor |
| Source stream | main |
| Message format string | The WLAN Gateway IOM <i>\$tmnxCardSlotNum\$</i> of group <i>\$tmnxWlanGwGrpId\$</i> is now <i>\$tmnxWlanGwTrue\$</i> . |
| Cause | The tmnxWlanGwlomActive notification is sent when the value of the object tmnxWlanGwlomOperState 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 1992: 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 1993: 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 <i>\$tmnxWlanGwMgwRestartCount\$</i> . |
| 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 1994: 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 <i>\$tmnxWlanGwMgw State\$</i> . |
| 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 1995: 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 (<i>\$tmnxWlanGwNumGw\$</i>) is high (<i>\$tmnxWlanGwNotifyTrue\$</i>). |
| 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 1996: *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 <i>\$tmnxWlanGwNotify3gppRelease\$</i> in the RADIUS Negotiated QoS profile, and the interface type <i>\$tmnxWlanGwMgwInterfaceType\$</i> 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 <i>tmnxWlanGwPgwTable</i> or the <i>tmnxWlanGwGgsnTable</i> of the conceptual row corresponding to the row in the <i>tmnxWlanGwMgwAddrTable</i> that matches the WLAN are used instead. |
| Recovery | The RADIUS Server configuration should be corrected. |

84.13 tmnxWlanGwResrcProblemCause

Table 1997: 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 | <i>\$tmnxWlanGwNotifyDescription\$</i> . |
| 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 1998: 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 <i>\$tmnxWlanGwResrcProblem\$</i> . |

| 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 tmnxWlanGwSubIfPmAddNewPIFailed

Table 1999: tmnxWlanGwSubIfPmAddNewPIFailed properties

| Property name | Value |
|----------------------------------|--|
| Application name | WLAN_GW |
| Event ID | 2015 |
| Event name | tmnxWlanGwSubIfPmAddNewPIFailed |
| 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 \$tmnxWlanGwNotifyAddrFamily\$) |
| 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 2000: 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 \$svclD\$, interface \$tmnxWlanGwSubIfIpsSubIfIndex\$, address \$tmnxWlanGwSubIfIpsSubnetAddr\$, prefix-length \$tmnxWlanGwSubIfIpsSubnetPrefLen\$, address-family \$tmnxWlanGwNotifyAddrFamily\$, description \$tmnxWlanGwNotifyDescription\$) |
| 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 2001: 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 tmnxWlanGwSubIfPmNewPIReqFailed

Table 2002: tmnxWlanGwSubIfPmNewPIReqFailed properties

| Property name | Value |
|----------------------------------|---|
| Application name | WLAN_GW |
| Event ID | 2014 |
| Event name | tmnxWlanGwSubIfPmNewPIReqFailed |
| 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 2003: 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. (svclId \$svclId\$, subflIndex \$tmnxWlanGwNotifySubflIndex\$, addrFamily \$tmnxWlanGwNotifyAddrFamily\$, isaGrpld \$tmnxWlanGwNotifyIsaGrpld\$, 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 tmnxWlanGwSublfPmPoolTimeout

Table 2004: tmnxWlanGwSublfPmPoolTimeout properties

| Property name | Value |
|----------------------------------|---|
| Application name | WLAN_GW |
| Event ID | 2017 |
| Event name | tmnxWlanGwSublfPmPoolTimeout |
| 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 tmnxWlanGwSublfPmPoolUsageLow

Table 2005: *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 <i>\$tmnxWlanGwNotifyAddrFamily\$</i>) |
| Cause | Pool usage dropped below 1%. |
| Effect | The pool has become stale. |
| Recovery | Manually clear the pool. |

84.22 tmnxWlanGwSubIfPmStartD6cFailed

Table 2006: *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 <i>\$svcId\$</i> , interface <i>\$tmnxWlanGwNotifySubIfIndex\$</i> , address-family <i>\$tmnxWlanGwNotifyAddrFamily\$</i>) |
| 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 2007: 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 2008: 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 <code>tmnxWlanGwIsaMemberTuQosProblem</code> has changed to <code>\$tmnxWlanGwIsaMemberTuQosProblem\$</code> . |
| 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 2009: *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 <code>\$tmnxWlanGwNotifyUeMacAddress\$</code> . |
| Cause | The system issues the <code>tmnxWlanGwUeCreationFail</code> notification when the creation of a WLAN Gateway UE in <code>tmnxWlanGwUeTable</code> 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 2010: 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 2011: 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 - \$tmnxWppNotifyDescription\$. |
| 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 2012: *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 <i>\$tmnxWppPortalGroupName\$</i> , address <i>\$tmnxWppPGHostAddr\$</i>) could not be authenticated - <i>\$tmnxWppNotifyDescription\$</i> . |
| 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 2013: *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 <i>\$tmnxWppPortalGroupName\$</i> has changed to (controlled router = <i>\$tmnxWppPortalGroupStateContrRtr\$</i> , number of interfaces = <i>\$tmnxWppPortalGroupStateNumItfs\$</i>). |
| 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 2014: 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 <i>\$tmnxWppPortalName\$</i> in router <i>\$vRtrID\$</i> has changed to (controlled router = <i>\$tmnxWppPortalStateControlledRtr\$</i> , number of interfaces = <i>\$tmnxWppPortalStateNumInterfaces\$</i>). |
| 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 2015: *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 <i>\$vRtrID\$</i> , portal <i>\$tmnxWppPortalName\$</i>) is unreachable - <i>\$tmnxWppNotifyDescription\$</i> . |
| 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

A

alulpTransportStateChanged: SVCNMR 1068
 alxDot1xHostAuthEvent: DOT1X 369
 apsEventChannelMismatch: APS 66
 apsEventFEPLF: APS 66
 apsEventModeMismatch: APS 67
 apsEventPSBF: APS 68
 apsEventSwitchover: APS 68
 asyncOperationStatusChange: MGMT_CORE 627
 authenticationFailure: SNMP 1038
 autoNodeProv: AUTO_PROV 76

B

bgpBackwardTransNotification: BGP 85
 bgpCfgViol: BGP 85
 bgpConnMgrTerminated: BGP 86
 bgpConnNoKA: BGP 86
 bgpConnNoOpenRcvd: BGP 87
 bgpEstablishedNotification: BGP 88
 bgpInterfaceDown: BGP 88
 bgpNoMemoryPeer: BGP 89
 bgpPeerNotFound: BGP 90
 bgpRejectConnBadLocAddr: BGP 90
 bgpRemoteEndClosedConn: BGP 91
 bgpTerminated: BGP 91
 bgpVariableRangeViolation: BGP 92

C

calltraceDebugEvent: CALLTRACE 112
 clearRTMError: IP 434
 cli_config_io: LI 508
 cli_config_io: USER 1274
 cli_unauth_config_io: LI 508
 cli_unauth_config_io: USER 1274
 cli_unauth_user_io: LI 509
 cli_unauth_user_io: USER 1275
 cli_user_io: LI 509
 cli_user_io: USER 1275
 cli_user_login_failed: LI 511
 cli_user_login_failed: SECURITY 920
 cli_user_login_failed: USER 1277
 cli_user_login_max_attempts: LI 511
 cli_user_login_max_attempts: SECURITY 921
 cli_user_login_max_attempts: USER 1277
 cli_user_login: LI 510
 cli_user_login: SECURITY 920
 cli_user_login: USER 1276
 cli_user_logout: LI 512
 cli_user_logout: SECURITY 922

cli_user_logout: USER 1278
 coldStart: SNMP 1038
 CpmlcPortSFFStatusDDMCorrupt: CHASSIS 118
 CpmlcPortSFFStatusFailure: CHASSIS 118
 CpmlcPortSFFStatusReadError: CHASSIS 119
 CpmlcPortSFFStatusUnsupported: CHASSIS 120

D

destinationDisabled: LI 513
 destinationDisabled: MIRROR 632
 destinationEnabled: LI 513
 destinationEnabled: MIRROR 632
 digitalDiagnosticMonitorCleared: PORT 806
 digitalDiagnosticMonitorFailed: PORT 806
 dot1agCfmFaultAlarm: ETH_CFM 381
 dot3OamNonThresholdEvent: EFM_OAM 371
 dot3OamThresholdEvent: EFM_OAM 371
 ds1AlarmClear: PORT 807
 ds1AlarmSet: PORT 808
 ds1LoopbackStart: PORT 808
 ds1LoopbackStop: PORT 809
 ds3AlarmClear: PORT 809
 ds3AlarmSet: PORT 810
 ds3LoopbackStart: PORT 811
 ds3LoopbackStop: PORT 811
 dsxClockSyncStateChange: PORT 812
 DynamicCostOff: LAG 490
 DynamicCostOn: LAG 490
 dynamicSdpBindConfigChanged: SVCNMR 1068
 dynamicSdpBindCreationFailed: SVCNMR 1069
 dynamicSdpConfigChanged: SVCNMR 1070
 dynamicSdpCreationFailed: SVCNMR 1070

E

eMplsIcmpSnpgMfibFailure: IGMP_SNOOPING 427
 enable_admin: SECURITY 922
 etherAlarmClear: PORT 812
 etherAlarmSet: PORT 813
 etherDuplexNotCompatible: PORT 814
 etherIngressRateCfgNotCompatible: PORT 814
 etherLoopCleared: PORT 815
 etherLoopDetected: PORT 816
 etherSpeedNotCompatible: PORT 816

F

fallingAlarm: SNMP 1039
 fibAddFailed: IP 434
 ftp_transfer_failed: SECURITY 923
 ftp_transfer_successful: SECURITY 924

ftp_user_login_failed: LI [514](#)
 ftp_user_login_failed: SECURITY [925](#)
 ftp_user_login_failed: USER [1279](#)
 ftp_user_login_max_attempts: LI [515](#)
 ftp_user_login_max_attempts: SECURITY [925](#)
 ftp_user_login_max_attempts: USER [1279](#)
 ftp_user_login: LI [514](#)
 ftp_user_login: SECURITY [924](#)
 ftp_user_login: USER [1278](#)
 ftp_user_logout: LI [516](#)
 ftp_user_logout: SECURITY [926](#)
 ftp_user_logout: USER [1280](#)

G

grpc_auth: LI [517](#)
 grpc_auth: SECURITY [927](#)
 grpc_unauth: LI [517](#)
 grpc_unauth: SECURITY [927](#)
 grpc_user_login_failed: LI [518](#)
 grpc_user_login_failed: SECURITY [929](#)
 grpc_user_login_failed: USER [1281](#)
 grpc_user_login_max_attempts: LI [519](#)
 grpc_user_login_max_attempts: SECURITY [929](#)
 grpc_user_login_max_attempts: USER [1282](#)
 grpc_user_login: LI [518](#)
 grpc_user_login: SECURITY [928](#)
 grpc_user_login: USER [1281](#)
 grpc_user_logout: LI [520](#)
 grpc_user_logout: SECURITY [930](#)
 grpc_user_logout: USER [1282](#)

H

higherPriorityBridge: STP [1048](#)
 host_snmp_attempts: LI [520](#)
 host_snmp_attempts: SECURITY [930](#)
 hostConnectivityLost: SVCMGR [1071](#)
 hostConnectivityRestored: SVCMGR [1072](#)

I

iesIfStatusChanged: SVCMGR [1072](#)
 ipAnyDuplicateAddress: IP [435](#)
 ipArpBadInterface: IP [435](#)
 ipArpDuplicateIpAddress: IP [436](#)
 ipArpDuplicateMacAddress: IP [437](#)
 ipArpInfoOverwritten: IP [437](#)
 ipDuplicateAddress: IP [438](#)
 ipEtherBroadcast: IP [439](#)

L

labelIndexAllocFailed: IP [439](#)
 LagPortAddFailed: LAG [491](#)
 LagPortAddFailureCleared: LAG [492](#)

LagStateEvent: LAG [492](#)
 LagSubGroupSelected: LAG [493](#)
 linkDown: SNMP [1040](#)
 linkUp: SNMP [1040](#)
 lldpRemTablesChange: LLDP [561](#)

M

mafEntryMatch: SECURITY [931](#)
 md_cli_io: LI [521](#)
 md_cli_io: SECURITY [932](#)
 md_cli_unauth_io: LI [522](#)
 md_cli_unauth_io: SECURITY [932](#)
 mdAutomaticRollbackFailed: MGMT_CORE [627](#)
 mdBofConfigChange: MGMT_CORE [628](#)
 mdCommitInProgress: SYSTEM [1210](#)
 mdCommitSucceeded: LI [522](#)
 mdCommitSucceeded: SYSTEM [1210](#)
 mdConfigChange: MGMT_CORE [629](#)
 mdDebugConfigChange: MGMT_CORE [629](#)
 mdLiConfigChange: LI [523](#)
 mdOcConfigChange: MGMT_CORE [630](#)
 mdRollbackFailed: MGMT_CORE [630](#)
 mdSaveCommitHistoryFailed: LI [523](#)
 mdSaveCommitHistoryFailed: SYSTEM [1211](#)
 mplsTunnelDown: MPLS [659](#)
 mplsTunnelReoptimized: MPLS [659](#)
 mplsTunnelRerouted: MPLS [660](#)
 mplsTunnelUp: MPLS [661](#)
 mplsXCDown: MPLS [661](#)
 mplsXCUp: MPLS [662](#)
 msapCreationFailure: SVCMGR [1073](#)
 msapStateChanged: SVCMGR [1073](#)
 msdpBackwardTransition: MSDP [688](#)
 msdpEstablished: MSDP [688](#)

N

netconf_auth: LI [524](#)
 netconf_auth: SECURITY [933](#)
 netconf_unauth: LI [525](#)
 netconf_unauth: SECURITY [934](#)
 netconf_user_login_failed: LI [526](#)
 netconf_user_login_failed: SECURITY [935](#)
 netconf_user_login_failed: USER [1284](#)
 netconf_user_login_max_attempts: LI [526](#)
 netconf_user_login_max_attempts: SECURITY [935](#)
 netconf_user_login_max_attempts: USER [1284](#)
 netconf_user_login: LI [525](#)
 netconf_user_login: SECURITY [934](#)
 netconf_user_login: USER [1283](#)
 netconf_user_logout: LI [527](#)
 netconf_user_logout: SECURITY [936](#)
 netconf_user_logout: USER [1285](#)
 newRootBridge: STP [1048](#)
 newRootSap: STP [1049](#)
 newRootVcpState: STP [1050](#)

O

otuAlarms: PORT [817](#)

P

persistenceRestoreProblem: SYSTEM [1212](#)
 persistencyClosedAlarmCleared: SYSTEM [1212](#)
 persistencyClosedAlarmRaised: SYSTEM [1213](#)
 persistencyEventReport: SYSTEM [1213](#)
 persistencyFileSysThresCleared: SYSTEM [1214](#)
 persistencyFileSysThresRaised: SYSTEM [1215](#)
 pipActiveProtocolChange: STP [1050](#)
 portError: PORT [817](#)

Q

qosNetworkPolicyMallocFailed: IP [440](#)

R

radiusFailed: LI [528](#)
 radiusInetServerOperStatusChange: SECURITY [937](#)
 radiusOperStatusChange: SECURITY [937](#)
 radiusSystemIpAddrNotSet: SECURITY [938](#)
 radiusUserProfileInvalid: SECURITY [939](#)
 receivedTCN: STP [1051](#)
 receiveNotification: BGP [93](#)
 ripPacketDiscarded: RIP [891](#)
 risingAlarm: SNMP [1041](#)

S

sapActiveProtocolChange: STP [1052](#)
 sapCemPacketDefectAlarm: SVCMMGR [1074](#)
 sapCemPacketDefectAlarmClear: SVCMMGR [1075](#)
 sapDcpDynamicConform: SECURITY [939](#)
 sapDcpDynamicEnforceAlloc: SECURITY [940](#)
 sapDcpDynamicEnforceFreed: SECURITY [941](#)
 sapDcpDynamicExcd: SECURITY [942](#)
 sapDcpDynamicHoldDownEnd: SECURITY [942](#)
 sapDcpDynamicHoldDownStart: SECURITY [943](#)
 sapDcpLocMonExcd: SECURITY [944](#)
 sapDcpLocMonExcdAllDynAlloc: SECURITY [945](#)
 sapDcpLocMonExcdAllDynFreed: SECURITY [945](#)
 sapDcpLocMonExcdDynResource: SECURITY [946](#)
 sapDcpStaticConform: SECURITY [947](#)
 sapDcpStaticExcd: SECURITY [948](#)
 sapDcpStaticHoldDownEnd: SECURITY [949](#)
 sapDcpStaticHoldDownStart: SECURITY [949](#)
 sapDHCPLseEntriesExceeded: DHCP [324](#)
 sapDHCPLseStateMobilityError: DHCP [324](#)
 sapDHCPLseStateOverride: DHCP [325](#)
 sapDHCPLseStatePopulateErr: DHCP [326](#)
 sapDHCPProxyServerError: DHCP [326](#)
 sapDHCPSuspiciousPcktRcvd: DHCP [327](#)

sapEncapDot1d: STP [1052](#)
 sapEncapPVST: STP [1053](#)
 sapEthLoopbackStarted: SVCMMGR [1075](#)
 sapEthLoopbackStopped: SVCMMGR [1076](#)
 sapHostBGPPeeringSetupFailed: SVCMMGR [1076](#)
 sapHostRipListenerSetupFailed: SVCMMGR [1077](#)
 sapIfIgnorePortStateStart: SVCMMGR [1078](#)
 sapIfIgnorePortStateStop: SVCMMGR [1078](#)
 sapIgmppSnpgGrpLimitExceeded: IGMP_SNOOPING [427](#)
 sapIgmppSnpgGrpSrcLimitExceeded: IGMP_SNOOPING [428](#)
 sapIgmppSnpgMcacPlyDropped: IGMP_SNOOPING [429](#)
 sapIgmppSnpgMcsFailure: IGMP_SNOOPING [429](#)
 sapIgmppSnpgSrcLimitExceeded: IGMP_SNOOPING [430](#)
 sapIpipeCelpAddrChange: SVCMMGR [1079](#)
 sapMldSnpgGrpLimitExceeded: MLD_SNOOPING [657](#)
 sapMldSnpgMcsFailure: MLD_SNOOPING [657](#)
 sapPortStateChangeProcessed: SVCMMGR [1080](#)
 sapReceivedPbbProtSrcMac: SVCMMGR [1080](#)
 sapReceivedProtSrcMac: SVCMMGR [1081](#)
 sapStatHost6DynMacConflict: DHCP [328](#)
 sapStaticHostDynMacConflict: DHCP [328](#)
 sapStatusChanged: SVCMMGR [1082](#)
 sapTlsDataSapInstStatusChgd: SVCMMGR [1082](#)
 sapTlsMacAddrLimitAlarmCleared: SVCMMGR [1083](#)
 sapTlsMacAddrLimitAlarmRaised: SVCMMGR [1084](#)
 sapTlsMacMoveExceeded: SVCMMGR [1084](#)
 sapTlsMacMoveExceedNonBlock: SVCMMGR [1085](#)
 sapTunnelEncapIpMtuTooSmall: SVCMMGR [1086](#)
 sapTunnelStateChange: SVCMMGR [1087](#)
 sbiBootConfig: SYSTEM [1215](#)
 sbiBootConfigFailFileError: SYSTEM [1216](#)
 sbiBootConfigOKFileError: SYSTEM [1217](#)
 sbiBootLiConfig: LI [528](#)
 sbiBootMdReadCommitHistoryFailed: LI [529](#)
 sbiBootMdReadCommitHistoryFailed: SYSTEM [1217](#)
 sbiBootSnmpd: SYSTEM [1218](#)
 schedActionFailure: SYSTEM [1218](#)
 sdhLoopbackStart: PORT [818](#)
 sdhLoopbackStop: PORT [819](#)
 sdpBandwidthOverbooked: SVCMMGR [1087](#)
 sdpBindDHCPLeaseEntriesExceeded: DHCP [329](#)
 sdpBindDHCPLeaseStateMobilityErr: DHCP [330](#)
 sdpBindDHCPLeaseStateOverride: DHCP [330](#)
 sdpBindDHCPLeaseStatePopulateErr: DHCP [331](#)
 sdpBindDHCPProxyServerError: DHCP [332](#)
 sdpBindDHCPSuspiciousPcktRcvd: DHCP [332](#)
 sdpBindEthLoopbackStarted: SVCMMGR [1088](#)
 sdpBindEthLoopbackStopped: SVCMMGR [1088](#)
 sdpBindInsufficientBandwidth: SVCMMGR [1089](#)
 sdpBindIpipeCelpAddressChange: SVCMMGR [1090](#)
 sdpBindPwLocalStatusBitsChanged: SVCMMGR [1090](#)
 sdpBindPwPeerFaultAddrChanged: SVCMMGR [1091](#)
 sdpBindPwPeerStatusBitsChanged: SVCMMGR [1092](#)
 sdpBindReceivedPbbProtSrcMac: SVCMMGR [1092](#)
 sdpBindReceivedProtSrcMac: SVCMMGR [1093](#)
 sdpBindSdpStateChangeProcessed: SVCMMGR [1094](#)
 sdpBindStatusChanged: SVCMMGR [1094](#)

sdpBindTIsMacMoveExceeded: SVCMMGR [1095](#)
 sdpBindTIsMacMoveExceedNonBlock: SVCMMGR [1096](#)
 sdpBndIgmPsnpgGrpLimitExceeded: IGMP_SNOOPING [431](#)
 sdpBndIgmPsnpgGrpSrcLimitExceed: IGMP_SNOOPING [431](#)
 sdpBndIgmPsnpgMcacPlyDropped: IGMP_SNOOPING [432](#)
 sdpBndIgmPsnpgSrcLimitExceeded: IGMP_SNOOPING [433](#)
 sdpBndMldSnpGGrpLimitExceeded: MLD_SNOOPING [658](#)
 sdpControlPwActiveStateChg: SVCMMGR [1097](#)
 sdpEgrlfsNetDomInconsCntChanged: SVCMMGR [1097](#)
 sdpKeepAliveLateReply: SVCMMGR [1098](#)
 sdpKeepAliveProbeFailure: SVCMMGR [1098](#)
 sdpKeepAliveStarted: SVCMMGR [1099](#)
 sdpKeepAliveStopped: SVCMMGR [1100](#)
 sdpPbbActvPwWithNonActvCtrlPwChg: SVCMMGR [1100](#)
 sdpStatusChanged: SVCMMGR [1101](#)
 sdpTIsMacAddrLimitAlarmCleared: SVCMMGR [1101](#)
 sdpTIsMacAddrLimitAlarmRaised: SVCMMGR [1102](#)
 sendNotification: BGP [93](#)
 SfmIcPortSFFStatusDDMCorrupt: CHASSIS [120](#)
 SfmIcPortSFFStatusFailure: CHASSIS [121](#)
 SfmIcPortSFFStatusReadError: CHASSIS [122](#)
 SfmIcPortSFFStatusUnsupported: CHASSIS [123](#)
 SFPInserted: PORT [819](#)
 SFPRemoved: PORT [820](#)
 SFPStatusBlocked: PORT [820](#)
 SFPStatusCulprit: PORT [821](#)
 SFPStatusDDMCorrupt: PORT [822](#)
 SFPStatusFailure: PORT [823](#)
 SFPStatusInvalidFormFactor: PORT [823](#)
 SFPStatusModuleFault: PORT [824](#)
 SFPStatusOperational: PORT [825](#)
 SFPStatusReadError: PORT [825](#)
 SFPStatusUnsupported: PORT [826](#)
 smScriptAbort: SYSTEM [1219](#)
 smScriptException: SYSTEM [1220](#)
 smScriptResult: SYSTEM [1220](#)
 snmp_user_set: LI [530](#)
 snmp_user_set: USER [1285](#)
 snmpdError: SNMP [1042](#)
 snptTimeDiffExceedsThreshold: SYSTEM [1221](#)
 socket_bind_failed: SYSTEM [1222](#)
 socket_conn_accept_failed: SYSTEM [1222](#)
 sonetSDHAlarmClear: PORT [827](#)
 sonetSDHAlarmSet: PORT [827](#)
 sonetSDHChannelAlarmClear: PORT [828](#)
 sonetSDHChannelAlarmSet: PORT [829](#)
 sourceDisabled: LI [530](#)
 sourceDisabled: MIRROR [633](#)
 sourceEnabled: LI [531](#)
 sourceEnabled: MIRROR [634](#)
 sourceIpFilterChange: MIRROR [634](#)
 sourceMacFilterChange: MIRROR [635](#)
 sourceSapChange: LI [532](#)
 sourceSapChange: MIRROR [636](#)
 sourceSubscriberChange: LI [532](#)
 sourceSubscriberChange: MIRROR [636](#)
 srrpPacketDiscarded: MC_REDUNDANCY [593](#)
 ssh_auth_key_gen: SECURITY [950](#)
 ssh_auth_key_synch_fail: SECURITY [951](#)
 SSH_server_preserve_key_fail: SECURITY [951](#)
 ssh_user_login_failed: LI [534](#)
 ssh_user_login_failed: SECURITY [952](#)
 ssh_user_login_max_attempts: LI [534](#)
 ssh_user_login_max_attempts: SECURITY [953](#)
 ssh_user_login: LI [533](#)
 ssh_user_login: SECURITY [952](#)
 ssh_user_logout: LI [535](#)
 ssh_user_logout: SECURITY [954](#)
 ssiSaveBackgroundConfigFailed: SYSTEM [1223](#)
 ssiSaveBackgroundConfigSucceeded: SYSTEM [1224](#)
 ssiSaveConfigFailed: LI [536](#)
 ssiSaveConfigFailed: SYSTEM [1224](#)
 ssiSaveConfigSucceeded: LI [536](#)
 ssiSaveConfigSucceeded: SYSTEM [1225](#)
 ssiSaveIncrementConfigFailed: SYSTEM [1225](#)
 ssiSaveIncrementConfigSucceeded: SYSTEM [1226](#)
 ssiSyncBootEnvFailed: SYSTEM [1227](#)
 ssiSyncBootEnvOK: SYSTEM [1227](#)
 ssiSyncCertFailed: SYSTEM [1228](#)
 ssiSyncCertOK: SYSTEM [1228](#)
 ssiSyncConfigFailed: LI [537](#)
 ssiSyncConfigFailed: SYSTEM [1229](#)
 ssiSyncConfigOK: LI [537](#)
 ssiSyncConfigOK: SYSTEM [1230](#)
 ssiSyncRollbackFailed: SYSTEM [1230](#)
 ssiSyncRollbackOK: SYSTEM [1231](#)
 STARTED: LOGGER [565](#)
 stiDateAndTimeChanged: SYSTEM [1231](#)
 stiDateAndTimeChanging: SYSTEM [1232](#)
 svcArpHostOverride: SVCMMGR [1103](#)
 svcArpHostPopulateErr: SVCMMGR [1103](#)
 svcBgpEvpnBHDupMacAddrsDetected: SVCMMGR [1104](#)
 svcBgpEvpnDupMacAddrsCleared: SVCMMGR [1105](#)
 svcBgpEvpnDupMacAddrsDetected: SVCMMGR [1105](#)
 svcBgpEvpnTepStateChgd: SVCMMGR [1106](#)
 svcBindSysHiUsageAlarmCleared: SVCMMGR [1106](#)
 svcBindSysHiUsageAlarmRaised: SVCMMGR [1107](#)
 svcDHCPLeaseStateRestoreProblem: DHCP [333](#)
 svcDHCPMiscellaneousProblem: DHCP [333](#)
 svcEndPointMacLimitAlarmCleared: SVCMMGR [1108](#)
 svcEndPointMacLimitAlarmRaised: SVCMMGR [1108](#)
 svcEpipePbbOperStatusChanged: SVCMMGR [1109](#)
 svcEPMCEPConfigMismatch: SVCMMGR [1110](#)
 svcEPMCEPConfigMismatchResolved: SVCMMGR [1110](#)
 svcEPMCEPPassiveModeActive: SVCMMGR [1111](#)
 svcEPMCEPPassiveModePassive: SVCMMGR [1112](#)
 svcEvpnESVxVTepLclBiasAddFailClr: SVCMMGR [1112](#)
 svcEvpnESVxVTepLclBiasAddFailSet: SVCMMGR [1113](#)
 svcEvpnEtreeBumLabelSysHiUsGClr: SVCMMGR [1114](#)
 svcEvpnEtreeBumLabelSysHiUsGSet: SVCMMGR [1114](#)
 svcEvpnMHAutoEsiConflict: SVCMMGR [1115](#)

svcEvpnMHAutoEsiCreated: [SVC MGR 1116](#)
 svcEvpnMHEsEviDFStateChgd: [SVC MGR 1116](#)
 svcEvpnMHEsIsidDFStateChgd: [SVC MGR 1117](#)
 svcEvpnMplsESDestTEPStateChgd: [SVC MGR 1118](#)
 svcEvpnMplsMacMoveExceedNonBlock: [SVC MGR 1118](#)
 svcEvpnMplsMldpESLbHiUsgClr: [SVC MGR 1119](#)
 svcEvpnMplsMldpESLbHiUsgSet: [SVC MGR 1120](#)
 svcEvpnMplsTEPEgrBndSvcHiUsgClr: [SVC MGR 1120](#)
 svcEvpnMplsTEPEgrBndSvcHiUsgSet: [SVC MGR 1121](#)
 svcEvpnMplsTEPEgrBndSysHiUsgClr: [SVC MGR 1122](#)
 svcEvpnMplsTEPEgrBndSysHiUsgSet: [SVC MGR 1122](#)
 svcEvpnMplsTEPEgrLbIStateChgd: [SVC MGR 1123](#)
 svcEvpnMplsTEPHiUsageCleared: [SVC MGR 1124](#)
 svcEvpnMplsTEPHiUsageRaised: [SVC MGR 1124](#)
 svcEvpnMplsTEPIpSysHiUsgClr: [SVC MGR 1125](#)
 svcEvpnMplsTEPIpSysHiUsgSet: [SVC MGR 1125](#)
 svcEvpnRcvdPbbProtSrcMac: [SVC MGR 1126](#)
 svcEvpnRcvdProtSrcMac: [SVC MGR 1127](#)
 svcEvpnVxInstESDStTEPStateChgd: [SVC MGR 1127](#)
 svcEvpnVxInstMHStandbyStatusChg: [SVC MGR 1128](#)
 svcEvpnVxVTepLclBiasAddFailClr: [SVC MGR 1129](#)
 svcEvpnVxVTepLclBiasAddFailSet: [SVC MGR 1129](#)
 svcFdbMimDestTblFullAlarm: [SVC MGR 1130](#)
 svcFdbMimDestTblFullAlarmCleared: [SVC MGR 1131](#)
 svcIdInvalid: [OAM 727](#)
 svcIdWrongType: [OAM 727](#)
 svcIcfSubForwardingStatsDisNotify: [SVC MGR 1131](#)
 svcIcfSubForwardingStatsEnNotify: [SVC MGR 1132](#)
 svcMSPwRetryExpiredNotif: [SVC MGR 1132](#)
 svcMSPwRtMisconfig: [SVC MGR 1133](#)
 svcOperGrpOperStatusChanged: [SVC MGR 1134](#)
 svcPersistencyProblem: [SVC MGR 1134](#)
 svcRestoreHostProblem: [SVC MGR 1135](#)
 svcRoutedVplsEvpnGWDStateChgd: [SVC MGR 1136](#)
 svcRvplsEvpnMcastDestSysHiUsgClr: [SVC MGR 1136](#)
 svcRvplsEvpnMcastDestSysHiUsgSet: [SVC MGR 1137](#)
 svcSiteMinDnTimerStateChg: [SVC MGR 1137](#)
 svcSrv6FunctionOutOfResources: [SVC MGR 1138](#)
 svcSrv6InstESDStTEPOperStateChgd: [SVC MGR 1139](#)
 svcSrv6InstTEPSidOperStateChgd: [SVC MGR 1139](#)
 svcSrv6TEPEgrBndSvcHiUsgClr: [SVC MGR 1140](#)
 svcSrv6TEPEgrBndSvcHiUsgSet: [SVC MGR 1141](#)
 svcSrv6TEPEgrBndSysHiUsgClr: [SVC MGR 1141](#)
 svcSrv6TEPEgrBndSysHiUsgSet: [SVC MGR 1142](#)
 svcStatusChanged: [SVC MGR 1143](#)
 svcSysEvpnESDfPrefOperValChange: [SVC MGR 1143](#)
 svcTlsEvpnTunnNHopHiUsgAlarmClr: [SVC MGR 1144](#)
 svcTlsEvpnTunnNHopHiUsgAlarmSet: [SVC MGR 1145](#)
 svcTlsFdbTableFullAlarmCleared: [SVC MGR 1145](#)
 svcTlsFdbTableFullAlarmRaised: [SVC MGR 1146](#)
 svcTlsGroupOperStatusChanged: [SVC MGR 1147](#)
 svcTlsMacPinningViolation: [SVC MGR 1147](#)
 svcTlsMfibTableFullAlarmCleared: [SVC MGR 1148](#)
 svcTlsMfibTableFullAlarmRaised: [SVC MGR 1148](#)
 svcTlsMrpAttrRegistrationFailed: [SVC MGR 1149](#)
 svcTlsMrpAttrTblFullAlarmCleared: [SVC MGR 1150](#)
 svcTlsMrpAttrTblFullAlarmRaised: [SVC MGR 1150](#)
 svcTlsProxyArpDupClear: [SVC MGR 1151](#)
 svcTlsProxyArpDupDetect: [SVC MGR 1151](#)
 svcTlsProxyArpSvcHiUsgClr: [SVC MGR 1152](#)
 svcTlsProxyArpSvcHiUsgSet: [SVC MGR 1153](#)
 svcTlsProxyArpSysHiUsgClr: [SVC MGR 1153](#)
 svcTlsProxyArpSysHiUsgSet: [SVC MGR 1154](#)
 svcTlsProxyArpUnauthorizedIP: [SVC MGR 1155](#)
 svcTlsProxyNdDupClear: [SVC MGR 1155](#)
 svcTlsProxyNdDupDetect: [SVC MGR 1156](#)
 svcTlsProxyNdSvcHiUsgClr: [SVC MGR 1157](#)
 svcTlsProxyNdSvcHiUsgSet: [SVC MGR 1157](#)
 svcTlsProxyNdSysHiUsgClr: [SVC MGR 1158](#)
 svcTlsProxyNdSysHiUsgSet: [SVC MGR 1158](#)
 svcTlsProxyNdUnauthorizedIP: [SVC MGR 1159](#)
 svcTlsSiteDesigFwdrChg: [SVC MGR 1160](#)
 svcTlsVTEPEgrVniSvcHiUsgAlarmClr: [SVC MGR 1160](#)
 svcTlsVTEPEgrVniSvcHiUsgAlarmSet: [SVC MGR 1161](#)
 svcTlsVTEPEgrVniSysHiUsgAlarmClr: [SVC MGR 1162](#)
 svcTlsVTEPEgrVniSysHiUsgAlarmSet: [SVC MGR 1162](#)
 svcTlsVTEPHiUsageAlarmCleared: [SVC MGR 1163](#)
 svcTlsVTEPHiUsageAlarmRaised: [SVC MGR 1163](#)
 svcTlsVxInstMacAdrLimitAlrmClrd: [SVC MGR 1164](#)
 svcTlsVxInstMacAdrLimitAlrmRsd: [SVC MGR 1165](#)
 svcTlsVxInstReplicatorChgd: [SVC MGR 1165](#)
 svcTlsVxInstVTEPEgrVniStateChgd: [SVC MGR 1166](#)
 svcVlSiteDesigFwdrChg: [SVC MGR 1167](#)
 svcVxlanEvpnMplsDestSysHiUsgClr: [SVC MGR 1167](#)
 svcVxlanEvpnMplsDestSysHiUsgSet: [SVC MGR 1168](#)
 syncOperationStatusChange: [MGMT_CORE 631](#)
 sysDNSSecFailedAuthentication: [SECURITY 954](#)

T

tacplusInetSrvrOperStatusChange: [SECURITY 955](#)
 tacplusOperStatusChange: [SECURITY 956](#)
 tacplusUserProfileInvalid: [SECURITY 956](#)
 tApsChannelMismatchClear: [APS 69](#)
 tApsChanTxLaisStateChange: [APS 69](#)
 tApsFEPLFClear: [APS 70](#)
 tApsLocalSwitchCommandClear: [APS 71](#)
 tApsLocalSwitchCommandSet: [APS 71](#)
 tApsMcApsCtlLinkStateChange: [APS 72](#)
 tApsModeMismatchClear: [APS 72](#)
 tApsPrimaryChannelChange: [APS 73](#)
 tApsPSBFClear: [APS 74](#)
 tApsRemoteSwitchCommandClear: [APS 74](#)
 tApsRemoteSwitchCommandSet: [APS 75](#)
 tBgp4PathAttrDiscarded: [BGP 94](#)
 tBgp4PathAttrInvalid: [BGP 95](#)
 tBgp4RouteInvalid: [BGP 96](#)
 tBgp4UpdateInvalid: [BGP 96](#)
 tBgp4WithdrawnRtFromUpdateError: [BGP 97](#)
 tBgpFibResourceFailPeer: [BGP 98](#)
 tBgpFlowspecUnsupportedComAction: [BGP 98](#)
 tBgpGeneral: [BGP 99](#)
 tBgpInstanceDynamicPeerLmtReachd: [BGP 100](#)
 tBgpInstConvStateTransition: [BGP 100](#)

tBgpMaxNgPfxLmt: BGP [101](#)
 tBgpMaxNgPfxLmtThresholdReached: BGP [101](#)
 tBgpNgBackwardTransition: BGP [102](#)
 tBgpNgEstablished: BGP [103](#)
 tBgpPeerGRStatusChange: BGP [103](#)
 tBgpPeerNgGRStatusChange: BGP [104](#)
 tBgpPeerNgHoldTimeInconsistent: BGP [105](#)
 tBgpPGDynamicPeerLmtReached: BGP [105](#)
 tBgpPGDynNbrfMaxSessLmtReachd: BGP [106](#)
 tBgpReceivedInvalidNlri: BGP [107](#)
 tChassisAirflowDirMismatch: CHASSIS [123](#)
 tChassisAirflowDirMismatchClr: CHASSIS [124](#)
 tChassisPowerSupplyMismatch: CHASSIS [125](#)
 tChassisPowerSupplyMismatchClr: CHASSIS [125](#)
 tChassisPowerSupplyUnsup: CHASSIS [126](#)
 tFilterApplyPathProblem: FILTER [395](#)
 tFilterBgpFlowSpecProblem: FILTER [395](#)
 tFilterEmbeddingOperStateChange: FILTER [396](#)
 tFilterEmbedFlowspecOperStateChg: FILTER [397](#)
 tFilterEmbedOpenflowOperStateChg: FILTER [398](#)
 tFilterOpenflowRequestRejected: FILTER [399](#)
 tFilterRadSharedFiltrAlarmClear: FILTER [399](#)
 tFilterRadSharedFiltrAlarmRaised: FILTER [400](#)
 tFilterRPActiveDestChangeEvent: FILTER [401](#)
 tFilterSubInsFiltrEntryDropped: FILTER [401](#)
 tFilterSubInsSpaceAlarmCleared: FILTER [402](#)
 tFilterSubInsSpaceAlarmRaised: FILTER [402](#)
 tFiltrLiRsvdBlockChangeEvent: LI [538](#)
 tIPFilterPBRPacketsDrop: FILTER [403](#)
 tipNbrAllocFailed: VRTR [1327](#)
 tIPsecBfdIntfSessStateChgd: IPSEC [441](#)
 tIPsecEsaVmMemHighWatermark: CHASSIS [127](#)
 tIPsecEsaVmMemLowWatermark: CHASSIS [127](#)
 tIPsecIslaMemHighWatermark: CHASSIS [128](#)
 tIPsecIslaMemLowWatermark: CHASSIS [128](#)
 tIPsecIslaMemMax: CHASSIS [129](#)
 tIPsecRadAcctPlyFailure: IPSEC [441](#)
 tIPsecRUSAFailToAddRoute: IPSEC [442](#)
 tIPsecRuTnlEncapIpMtuTooSmall: IPSEC [443](#)
 tIPsecRUTnlFailToCreate: IPSEC [443](#)
 tIPsecRUTnlRemoved: IPSEC [444](#)
 tIPsecTrustAnchorPrfOprChg: IPSEC [445](#)
 tIPsecTunnelEncapIpMtuTooSmall: IPSEC [445](#)
 tIPsecTunnelProtocolFailed: IPSEC [446](#)
 tLagAdaptiveLoadbalancingChanged: LAG [493](#)
 tLagMemberStateEvent: LAG [494](#)
 tMcIPsecDomainActivityStateChg: MC_REDUNDANCY [593](#)
 tMcIPsecDomainProtStatusChg: MC_REDUNDANCY [594](#)
 tMcPeerIPsecTnlGrpMasterStateChg: MC_REDUNDANCY [595](#)
 tMcPeerIPsecTnlGrpProtStatusChg: MC_REDUNDANCY [596](#)
 tMirrorDestinationChangeReject: LI [539](#)
 tMirrorFilterAssignToIftWarn: LI [539](#)
 tMirrorFilterAssignToSapWarn: LI [540](#)
 tMirrorFilterAssignToSdpWarn: LI [541](#)
 tMirrorFiltrUnavailSath: MIRROR [637](#)
 tMirrorFiltrUnavailSathClr: MIRROR [637](#)
 tMirrorLiFiltrUnavailSath: LI [541](#)
 tMirrorLiFiltrUnavailSathClr: LI [542](#)
 tMirrorLiNat64SubOperStateCh: LI [543](#)
 tMirrorLiNatL2awSubOperStateCh: LI [543](#)
 tMirrorLiNatLsnSubOperStateCh: LI [544](#)
 tMirrorLiPortUnavailSath: LI [545](#)
 tMirrorLiPortUnavailSathClr: LI [545](#)
 tMirrorLiSapUnavailSath: LI [546](#)
 tMirrorLiSapUnavailSathClr: LI [547](#)
 tMirrorLiSrcPortLicInvalid: LI [547](#)
 tMirrorLiUpleInvalid: LI [548](#)
 tMirrorLiUpSubFailed: LI [549](#)
 tMirrorLiUpSubSuccess: LI [549](#)
 tMirrorLiX2Alarm: LI [550](#)
 tMirrorLiXIfLicenseInvalid: LI [551](#)
 tMirrorLiXIfLicenseInvalid: SYSTEM [1233](#)
 tMirrorPortUnavailSath: MIRROR [638](#)
 tMirrorPortUnavailSathClr: MIRROR [639](#)
 tMirrorSapUnavailSath: MIRROR [639](#)
 tMirrorSapUnavailSathClr: MIRROR [640](#)
 tMirrorSourceFilterAssignReject: LI [551](#)
 tMirrorSourceFilterAssignWarn: LI [552](#)
 tMirrorSourceFilterOverruled: LI [553](#)
 tMirrorSourceIPFiltrChangeReject: LI [553](#)
 tMirrorSourceIpv6FilterChange: MIRROR [641](#)
 tMirrorSourceIpv6FiltrChangeRej: LI [554](#)
 tMirrorSourceLiFilterChanged: LI [555](#)
 tMirrorSourceLiSubProblem: LI [556](#)
 tMirrorSourceMacFiltrChangeReject: LI [556](#)
 tmnxAlarmInputVoltageFailure: CHASSIS [130](#)
 tmnxAncpEgrRateMonitorEvent: GSMP [405](#)
 tmnxAncpEgrRateMonitorEventL: GSMP [405](#)
 tmnxAncpIngRateMonitorEvent: GSMP [406](#)
 tmnxAncpIngRateMonitorEventL: GSMP [407](#)
 tmnxAncpLoopbackTestCompleted: OAM [728](#)
 tmnxAncpLoopbackTestCompletedL: OAM [728](#)
 tmnxAncpSesRejected: GSMP [407](#)
 tmnxAncpShcvDisabledEvent: GSMP [408](#)
 tmnxAncpShcvDisabledEventL: GSMP [409](#)
 tmnxAncpStringRejected: GSMP [409](#)
 tmnxAnySecMkaOperStateChanged: ANYSEC [14](#)
 tmnxAnySecMkaPskRollover: ANYSEC [14](#)
 tmnxAnySecMkaSessionEnded: ANYSEC [15](#)
 tmnxAnySecMkaSessionEstablished: ANYSEC [16](#)
 tmnxAnySecMkaSessionInitiation: ANYSEC [16](#)
 tmnxAnySecMkaSessionTermination: ANYSEC [17](#)
 tmnxAnySecPeerInconsisRxSciClrd: ANYSEC [18](#)
 tmnxAnySecPeerInconsisRxSciDtctd: ANYSEC [19](#)
 tmnxAnySecSessionDisabled: ANYSEC [19](#)
 tmnxAnySecSessionEnabled: ANYSEC [20](#)
 tmnxAppPkiCertVerificationFailed: SECURITY [957](#)
 tmnxBfdOnLspExtSessDeleted: BFD [77](#)
 tmnxBfdOnLspExtSessDown: BFD [77](#)
 tmnxBfdOnLspExtSessNoCpmNpResrcs: BFD [78](#)
 tmnxBfdOnLspExtSessProtChange: BFD [79](#)
 tmnxBfdOnLspExtSessUp: BFD [79](#)

tmnxBfdOnLspSessDeleted: BFD [80](#)
 tmnxBfdOnLspSessDown: BFD [81](#)
 tmnxBfdOnLspSessNoCpmNpResources: BFD [81](#)
 tmnxBfdOnLspSessNoTailResources: BFD [82](#)
 tmnxBfdOnLspSessProtChange: BFD [83](#)
 tmnxBfdOnLspSessUp: BFD [84](#)
 tmnxBluetoothModuleConnectionChg: CHASSIS [130](#)
 tmnxBmpSessionStatusChange: BGP [107](#)
 tmnxBsxAarpInstOperStateChanged:
 APPLICATION_ASSURANCE [22](#)
 tmnxBsxAarpInstStateChanged:
 APPLICATION_ASSURANCE [22](#)
 tmnxBsxAaSubPolResExceeded:
 APPLICATION_ASSURANCE [23](#)
 tmnxBsxAaSubPolResExceededClear:
 APPLICATION_ASSURANCE [24](#)
 tmnxBsxAaSubscriberAcctDataLoss:
 APPLICATION_ASSURANCE [24](#)
 tmnxBsxAaSubscribersUnassigned:
 APPLICATION_ASSURANCE [25](#)
 tmnxBsxCertProfileOperStateChngd:
 APPLICATION_ASSURANCE [26](#)
 tmnxBsxDatapathCpuUsage: APPLICATION_ASSURANCE
[26](#)
 tmnxBsxDatapathCpuUsageClear:
 APPLICATION_ASSURANCE [27](#)
 tmnxBsxDnsIpCacheFull: APPLICATION_ASSURANCE [28](#)
 tmnxBsxDnsIpCacheFullClear:
 APPLICATION_ASSURANCE [28](#)
 tmnxBsxHttpUriParamLimitExceeded:
 APPLICATION_ASSURANCE [29](#)
 tmnxBsxIsaAaGrpBitRate: APPLICATION_ASSURANCE [30](#)
 tmnxBsxIsaAaGrpBitRateClear:
 APPLICATION_ASSURANCE [31](#)
 tmnxBsxIsaAaGrpCapCostThres:
 APPLICATION_ASSURANCE [31](#)
 tmnxBsxIsaAaGrpCapCostThresClear:
 APPLICATION_ASSURANCE [32](#)
 tmnxBsxIsaAaGrpFailureClearV2:
 APPLICATION_ASSURANCE [33](#)
 tmnxBsxIsaAaGrpFailureV2: APPLICATION_ASSURANCE
[33](#)
 tmnxBsxIsaAaGrpFlowFull: APPLICATION_ASSURANCE [34](#)
 tmnxBsxIsaAaGrpFlowFullClear:
 APPLICATION_ASSURANCE [35](#)
 tmnxBsxIsaAaGrpFlowSetup: APPLICATION_ASSURANCE
[35](#)
 tmnxBsxIsaAaGrpFlowSetupClear:
 APPLICATION_ASSURANCE [36](#)
 tmnxBsxIsaAaGrpFmSbWaSBufOvld:
 APPLICATION_ASSURANCE [37](#)
 tmnxBsxIsaAaGrpFmSbWaSBufOvldClr:
 APPLICATION_ASSURANCE [37](#)
 tmnxBsxIsaAaGrpNonRedundantV2:
 APPLICATION_ASSURANCE [38](#)
 tmnxBsxIsaAaGrpOvridCutthru:
 APPLICATION_ASSURANCE [39](#)
 tmnxBsxIsaAaGrpOvridCutthruClr:
 APPLICATION_ASSURANCE [39](#)
 tmnxBsxIsaAaGrpPacketRate:
 APPLICATION_ASSURANCE [40](#)
 tmnxBsxIsaAaGrpPacketRateClear:
 APPLICATION_ASSURANCE [41](#)
 tmnxBsxIsaAaGrpSwitchover: APPLICATION_ASSURANCE
[41](#)
 tmnxBsxIsaAaGrpToSbWaSBufOvld:
 APPLICATION_ASSURANCE [42](#)
 tmnxBsxIsaAaGrpToSbWaSBufOvldClr:
 APPLICATION_ASSURANCE [43](#)
 tmnxBsxIsaAaSubLoadBalance:
 APPLICATION_ASSURANCE [43](#)
 tmnxBsxIsaAaTimFileProcFailure:
 APPLICATION_ASSURANCE [44](#)
 tmnxBsxMobileSubModifyFailure:
 APPLICATION_ASSURANCE [45](#)
 tmnxBsxRadApFailure: APPLICATION_ASSURANCE [45](#)
 tmnxBsxRadApIntrmUpdateSkipped:
 APPLICATION_ASSURANCE [46](#)
 tmnxBsxRadApServOperStateChange:
 APPLICATION_ASSURANCE [47](#)
 tmnxBsxStatFtrEnTcaThreshCrClear:
 APPLICATION_ASSURANCE [47](#)
 tmnxBsxStatFtrEnTcaThreshCrossed:
 APPLICATION_ASSURANCE [48](#)
 tmnxBsxStatFtrTcaThreshCrClear:
 APPLICATION_ASSURANCE [49](#)
 tmnxBsxStatFtrTcaThreshCrossed:
 APPLICATION_ASSURANCE [50](#)
 tmnxBsxStatPolcrTcaThreshCrClear:
 APPLICATION_ASSURANCE [50](#)
 tmnxBsxStatPolcrTcaThreshCrossed:
 APPLICATION_ASSURANCE [51](#)
 tmnxBsxStatTcaThreshCrossed:
 APPLICATION_ASSURANCE [52](#)
 tmnxBsxStatTcaThreshCrossedClear:
 APPLICATION_ASSURANCE [52](#)
 tmnxBsxSubModifyFailure: APPLICATION_ASSURANCE [53](#)
 tmnxBsxSubQuarantined: APPLICATION_ASSURANCE [54](#)
 tmnxBsxSubQuarantinedClear:
 APPLICATION_ASSURANCE [54](#)
 tmnxBsxTcpValTcaCrossed: APPLICATION_ASSURANCE
[55](#)
 tmnxBsxTcpValTcaCrossedClear:
 APPLICATION_ASSURANCE [56](#)
 tmnxBsxTransIpPolAaSubCreated:
 APPLICATION_ASSURANCE [57](#)
 tmnxBsxTransIpPolAaSubDeleted:
 APPLICATION_ASSURANCE [57](#)
 tmnxBsxTransIpPolDhcpAddWarning:
 APPLICATION_ASSURANCE [58](#)
 tmnxBsxTransIpPolDhcpDelWarning:
 APPLICATION_ASSURANCE [59](#)
 tmnxBsxTransIpPolDiamGxError:
 APPLICATION_ASSURANCE [59](#)

tmnxBsxTransIpPolRadCoAAudit:
 APPLICATION_ASSURANCE 60
 tmnxBsxTransIpPolRadCoAError:
 APPLICATION_ASSURANCE 61
 tmnxBsxTransIpPolRadDiscError:
 APPLICATION_ASSURANCE 61
 tmnxBsxTransitIpPersistenceWarn:
 APPLICATION_ASSURANCE 62
 tmnxBsxUrlFilterOperStateChange:
 APPLICATION_ASSURANCE 63
 tmnxBsxUrlFtrWebServOprStateChg:
 APPLICATION_ASSURANCE 63
 tmnxBsxUrlListFailure: APPLICATION_ASSURANCE 64
 tmnxBsxUrlListUpdate: APPLICATION_ASSURANCE 65
 tmnxCallTraceLocSizeLimitReached: CALLTRACE 112
 tmnxCallTraceMaxFilesNumReached: CALLTRACE 113
 tmnxCAPProfileStateChange: SECURITY 958
 tmnxCAPProfUpDueToRevokeChkCriOpt: SECURITY 958
 tmnxCardResMacFdbHighUsgClr: CHASSIS 131
 tmnxCardResMacFdbHighUsgSet: CHASSIS 132
 tmnxCellPortCbsdAuthorized: PORT 829
 tmnxCellPortCbsdGranted: PORT 830
 tmnxCellPortCbsdRegistered: PORT 831
 tmnxCellPortCbsdTransDown: PORT 831
 tmnxCellPortCbsdUnregistered: PORT 832
 tmnxCellularActiveSimChange: PORT 833
 tmnxCellularBearerCreated: PORT 833
 tmnxCellularBearerDeleted: PORT 834
 tmnxCellularBearerModified: PORT 834
 tmnxCellularNoServiceReset: PORT 835
 tmnxCellularRssiAlarm: PORT 836
 tmnxCellularRssiAlarmClear: PORT 836
 tmnxCertExport: SECURITY 959
 tmnxCertImport: SECURITY 960
 tmnxCertKeyPairGen: SECURITY 960
 tmnxCflowdCreateFailure: CFLOWD 115
 tmnxCflowdFlowCreateFailure: CFLOWD 115
 tmnxCflowdPacketTxFailure: CFLOWD 116
 tmnxCflowdStateChange: CFLOWD 116
 tmnxChassisAntiTheftModeBoot: CHASSIS 132
 tmnxChassisAntiTheftUnlocked: CHASSIS 133
 tmnxChassisGoldenStatusEvent: CHASSIS 134
 tmnxChassisHiBwMcastAlarm: CHASSIS 134
 tmnxChassisNotificationClear: CHASSIS 135
 tmnxChassisUpgradeComplete: CHASSIS 135
 tmnxChassisUpgradeInProgress: CHASSIS 136
 tmnxClear: LI 557
 tmnxClear: LOGGER 565
 tmnxCliGroupSessionLimitExceeded: SECURITY 961
 tmnxConfigConflict: SYSTEM 1233
 tmnxConfigCreate: LI 558
 tmnxConfigCreate: SECURITY 962
 tmnxConfigCreate: SYSTEM 1234
 tmnxConfigDelete: LI 558
 tmnxConfigDelete: SECURITY 963
 tmnxConfigDelete: SYSTEM 1235
 tmnxConfigModify: LI 559
 tmnxConfigModify: SECURITY 963
 tmnxConfigModify: SYSTEM 1235
 tmnxCpmALocalIcPortAvail: CHASSIS 137
 tmnxCpmANoLocalIcPort: CHASSIS 137
 tmnxCpmBLocalIcPortAvail: CHASSIS 138
 tmnxCpmBNoLocalIcPort: CHASSIS 139
 tmnxCpmCardSyncFileNotPresent: CHASSIS 140
 tmnxCpmIcPortDDMClear: CHASSIS 140
 tmnxCpmIcPortDDMFailure: CHASSIS 141
 tmnxCpmIcPortDown: CHASSIS 142
 tmnxCpmIcPortSFFInserted: CHASSIS 142
 tmnxCpmIcPortSFFRemoved: CHASSIS 143
 tmnxCpmIcPortUp: CHASSIS 144
 tmnxCpmMemSizeMismatch: CHASSIS 144
 tmnxCpmMemSizeMismatchClear: CHASSIS 145
 tmnxCpmProtDefPolModified: SECURITY 964
 tmnxCpmProtExcdSapEcm: SECURITY 965
 tmnxCpmProtExcdSapIpl: SECURITY 965
 tmnxCpmProtExcdSdpBind: SECURITY 966
 tmnxCpmProtExcdSdpBindEcm: SECURITY 967
 tmnxCpmProtExcdSdpBindIpl: SECURITY 968
 tmnxCpmProtViolIfl: SECURITY 968
 tmnxCpmProtViolIflOutProf: SECURITY 969
 tmnxCpmProtViolMac: SECURITY 970
 tmnxCpmProtViolPort: SECURITY 971
 tmnxCpmProtViolPortAgg: SECURITY 972
 tmnxCpmProtViolSap: SECURITY 972
 tmnxCpmProtViolSapOutProf: SECURITY 973
 tmnxCpmProtViolSdpBind: SECURITY 974
 tmnxCpmProtViolSdpBindOutProf: SECURITY 975
 tmnxCpmProtViolVdoSvcClient: SECURITY 975
 tmnxCpmProtViolVdoVrtrClient: SECURITY 976
 tmnxCustomEvent1: LOGGER 566
 tmnxCustomEvent2: LOGGER 567
 tmnxCustomEvent3: LOGGER 567
 tmnxCustomEvent4: LOGGER 568
 tmnxCustomEvent5: LOGGER 568
 tmnxCustomEvent6: LOGGER 569
 tmnxDcpCardFpEventOvrflw: CHASSIS 146
 tmnxDcpCardFpEventOvrflw: SECURITY 977
 tmnxDcpCardFpEventOvrflwClr: CHASSIS 146
 tmnxDcpCardFpEventOvrflwClr: SECURITY 977
 tmnxDcpCardSapEventOvrflw: CHASSIS 147
 tmnxDcpCardSapEventOvrflw: SECURITY 978
 tmnxDcpCardSapEventOvrflwClr: CHASSIS 148
 tmnxDcpCardSapEventOvrflwClr: SECURITY 978
 tmnxDcpCardVrtrIflEventOvrflw: CHASSIS 148
 tmnxDcpCardVrtrIflEventOvrflw: SECURITY 979
 tmnxDcpCardVrtrIflEventOvrflwClr: CHASSIS 149
 tmnxDcpCardVrtrIflEventOvrflwClr: SECURITY 980
 tmnxDcpFpDynPoolUsageHiAlmClear: CHASSIS 150
 tmnxDcpFpDynPoolUsageHiAlmClear: SECURITY 980
 tmnxDcpFpDynPoolUsageHiAlmRaise: CHASSIS 150
 tmnxDcpFpDynPoolUsageHiAlmRaise: SECURITY 981
 tmnxDhcpsAddrAllocationFailure: DHCP 341
 tmnxDhcpsFoLeaseUpdateFailed: DHCP 341
 tmnxDhcpsFoStateChange: DHCP 342

tmnxDhcpsLeaseOfferedExpired: DHCPDS 343
 tmnxDhcpsPacketDropped: DHCPDS 344
 tmnxDhcpsPoolFoLeaseUpdateFailed: DHCPDS 345
 tmnxDhcpsPoolFoStateChange: DHCPDS 345
 tmnxDhcpSvrDeclineStaticAddr: DHCPDS 346
 tmnxDhcpSvrHostConflict: DHCPDS 347
 tmnxDhcpSvrIntLseConflict: DHCPDS 348
 tmnxDhcpSvrLeaseCreate: DHCPDS 348
 tmnxDhcpSvrLeaseDefaultTimers: DHCPDS 349
 tmnxDhcpSvrLeaseDelete: DHCPDS 350
 tmnxDhcpSvrLeaseModify: DHCPDS 350
 tmnxDhcpSvrLeaseNotOwner: DHCPDS 351
 tmnxDhcpSvrMaxLeasesReached: DHCPDS 352
 tmnxDhcpSvrMsgTooLong: DHCPDS 353
 tmnxDhcpSvrNoContFreeBlocks: DHCPDS 353
 tmnxDhcpSvrNoSubnetFixAddr: DHCPDS 354
 tmnxDhcpSvrPfxThDepletedV6: DHCPDS 355
 tmnxDhcpSvrPfxThTooLowV6: DHCPDS 356
 tmnxDhcpSvrPIThDepletedV6: DHCPDS 356
 tmnxDhcpSvrPIThTooLowV6: DHCPDS 357
 tmnxDhcpSvrPoolDepleted: DHCPDS 358
 tmnxDhcpSvrPoolMinFreeExc: DHCPDS 359
 tmnxDhcpSvrPoolUnknown: DHCPDS 359
 tmnxDhcpSvrSubnetDepleted: DHCPDS 360
 tmnxDhcpSvrSubnetMinFreeExc: DHCPDS 361
 tmnxDhcpSvrUserDbUnknown: DHCPDS 361
 tmnxDiamAppSessionFailure: DIAMETER 364
 tmnxDiamMessageDropped: DIAMETER 364
 tmnxDiamNdPeerStatActiveChanged: DIAMETER 365
 tmnxDiamPolicyPeerStateChange: DIAMETER 366
 tmnxDiamPpPrxMcLocStateChange: DIAMETER 366
 tmnxDiamSessionEvent: DIAMETER 367
 tmnxDiscoveryCellularReq: ADP 12
 tmnxDiscoveryEndNotify: ADP 12
 tmnxDot1agCfmMepAisStateChange: ETH_CFM 382
 tmnxDot1agCfmMepCsfStateChange: ETH_CFM 382
 tmnxDot1agCfmMepDMTestComplete: ETH_CFM 383
 tmnxDot1agCfmMepEthTestComplete: ETH_CFM 384
 tmnxDot1agCfmMepFcltyFaultClear: ETH_CFM 384
 tmnxDot1agCfmMepFcltyFaultRaise: ETH_CFM 385
 tmnxDot1agCfmMepLbmTestComplete: ETH_CFM 386
 tmnxDot1agCfmMepLtmTestComplete: ETH_CFM 386
 tmnxDot1agCfmMepOperGrpStateChgd: ETH_CFM 387
 tmnxDot1agCfmMepSLMTestComplete: ETH_CFM 388
 tmnxDot1agCfmMipEvaluation: ETH_CFM 389
 tmnxDot3OamLoopCleared: EFM_OAM 372
 tmnxDot3OamLoopDetected: EFM_OAM 373
 tmnxDot3OamNonThresholdEventClr: EFM_OAM 373
 tmnxDot3OamPeerChanged: EFM_OAM 374
 tmnxDot3OamSdThresholdEvent: EFM_OAM 375
 tmnxDot3OamThresholdEventClr: EFM_OAM 376
 tmnxDS0ChanGrpLoopbackStarted: PORT 837
 tmnxDS0ChanGrpLoopbackStopped: PORT 838
 tmnxDynSvcSapFailed: DYNVSC 370
 tmnxEhsDroppedByMinDelay: SYSTEM 1236
 tmnxEhsHandlerInvoked: SYSTEM 1237
 tmnxElmiEVCStatusChangeEvent: ELMI 377
 tmnxElmilfStatusChangeEvent: ELMI 377
 tmnxEndPointTxActiveChanged: SVCMGR 1169
 tmnxEnvTempTooHigh: CHASSIS 151
 tmnxEqBpEpromFail: CHASSIS 152
 tmnxEqBpEpromFailClear: CHASSIS 152
 tmnxEqBpEpromWarning: CHASSIS 153
 tmnxEqBpEpromWarningClear: CHASSIS 153
 tmnxEqCardChipIfCellEvent: CHASSIS 154
 tmnxEqCardChipIfDownEvent: CHASSIS 155
 tmnxEqCardFailure: CHASSIS 156
 tmnxEqCardFirmwareUpgraded: CHASSIS 156
 tmnxEqCardInserted: CHASSIS 157
 tmnxEqCardMissing: CHASSIS 158
 tmnxEqCardMissingClear: CHASSIS 158
 tmnxEqCardPChipCamEvent: CHASSIS 159
 tmnxEqCardPChipError: CHASSIS 160
 tmnxEqCardPChipMemoryEvent: CHASSIS 160
 tmnxEqCardQChipBufMemoryEvent: CHASSIS 161
 tmnxEqCardQChipIntMemoryEvent: CHASSIS 162
 tmnxEqCardQChipStatsMemoryEvent: CHASSIS 162
 tmnxEqCardRemoved: CHASSIS 163
 tmnxEqCardSoftResetAlarm: CHASSIS 164
 tmnxEqCardTChipParityEvent: CHASSIS 164
 tmnxEqCohOptPortAlarm: PORT 839
 tmnxEqDataPathFailureProtImpact: CHASSIS 165
 tmnxEqEsaHostPortCrcAlarm: CHASSIS 166
 tmnxEqEsaHostPortCrcAlarmClear: CHASSIS 166
 tmnxEqFlashDataLoss: CHASSIS 167
 tmnxEqFlashDiskFull: CHASSIS 168
 tmnxEqFpgaSoftError: CHASSIS 168
 tmnxEqHwEnhancedCapability: CHASSIS 169
 tmnxEqHwEventDetected: CHASSIS 170
 tmnxEqLowPowerSwFabModeDisabled: CHASSIS 170
 tmnxEqLowPowerSwFabModeEnabled: CHASSIS 171
 tmnxEqLowSwitchFabricCap: CHASSIS 171
 tmnxEqLowSwitchFabricCapClear: CHASSIS 172
 tmnxEqMdaCfgNotCompatible: CHASSIS 173
 tmnxEqMdaIngrXplError: CHASSIS 173
 tmnxEqMdaSyncENotCompatible: CHASSIS 174
 tmnxEqMdaXplError: CHASSIS 175
 tmnxEqMgmtEthRedStandbyClear: CHASSIS 175
 tmnxEqMgmtEthRedStandbyRaise: CHASSIS 176
 tmnxEqOperStateChange: CHASSIS 177
 tmnxEqPhysChassisFanFailure: CHASSIS 178
 tmnxEqPhysChassisFanFailureClear: CHASSIS 178
 tmnxEqPhysChassPowerSupAcFail: CHASSIS 179
 tmnxEqPhysChassPowerSupAcFailClr: CHASSIS 179
 tmnxEqPhysChassPowerSupDcFail: CHASSIS 180
 tmnxEqPhysChassPowerSupDcFailClr: CHASSIS 181
 tmnxEqPhysChassPowerSupInFail: CHASSIS 181
 tmnxEqPhysChassPowerSupInFailClr: CHASSIS 182
 tmnxEqPhysChassPowerSupOutFail: CHASSIS 183
 tmnxEqPhysChassPowerSupOutFailClr: CHASSIS 183
 tmnxEqPhysChassPowerSupOvrTmp: CHASSIS 184
 tmnxEqPhysChassPowerSupOvrTmpClr: CHASSIS 184
 tmnxEqPortEtherCrcAlarm: PORT 839
 tmnxEqPortEtherCrcAlarmClear: PORT 840

tmnxEqPortEtherEgressRateChange: PORT [841](#)
 tmnxEqPortEtherInternalAlarm: PORT [841](#)
 tmnxEqPortEtherInternalAlarmClr: PORT [842](#)
 tmnxEqPortEtherSymMonAlarm: PORT [843](#)
 tmnxEqPortEtherSymMonAlarmClear: PORT [843](#)
 tmnxEqPortFlexEGroupAlarm: PORT [844](#)
 tmnxEqPortFlexEGroupAlarmClr: PORT [845](#)
 tmnxEqPortFlexEMbrPhyInstAlarm: PORT [845](#)
 tmnxEqPortFlexEMbrPhyInstAlarmClr: PORT [846](#)
 tmnxEqPortFlexEMemberAlarm: PORT [846](#)
 tmnxEqPortFlexEMemberAlarmClr: PORT [847](#)
 tmnxEqPowerCapacityExceeded: CHASSIS [185](#)
 tmnxEqPowerCapacityExceededClear: CHASSIS [186](#)
 tmnxEqPowerLostCapacity: CHASSIS [186](#)
 tmnxEqPowerLostCapacityClear: CHASSIS [187](#)
 tmnxEqPowerOverloadState: CHASSIS [188](#)
 tmnxEqPowerOverloadStateClear: CHASSIS [188](#)
 tmnxEqPowerSafetyAlertClear: CHASSIS [189](#)
 tmnxEqPowerSafetyAlertThreshold: CHASSIS [190](#)
 tmnxEqPowerSafetyLevelClear: CHASSIS [190](#)
 tmnxEqPowerSafetyLevelThreshold: CHASSIS [191](#)
 tmnxEqPowerSupplyInserted: CHASSIS [192](#)
 tmnxEqPowerSupplyRemoved: CHASSIS [192](#)
 tmnxEqProvPowerCapacityAlm: CHASSIS [193](#)
 tmnxEqProvPowerCapacityAlmClr: CHASSIS [194](#)
 tmnxEqSonetClockSrcNotCompatible: PORT [848](#)
 tmnxEqSonetFramingNotCompatible: PORT [848](#)
 tmnxEqSonetSfThreshNotCompatible: PORT [849](#)
 tmnxEqSyncIfTimingBITS2Alarm: CHASSIS [194](#)
 tmnxEqSyncIfTimingBITS2AlarmClr: CHASSIS [195](#)
 tmnxEqSyncIfTimingBITS2Quality: CHASSIS [196](#)
 tmnxEqSyncIfTimingBITSAlarm: CHASSIS [196](#)
 tmnxEqSyncIfTimingBITSAlarmClear: CHASSIS [197](#)
 tmnxEqSyncIfTimingBITSOutRefChg: CHASSIS [197](#)
 tmnxEqSyncIfTimingBITSQuality: CHASSIS [198](#)
 tmnxEqSyncIfTimingGnss2Alarm: CHASSIS [199](#)
 tmnxEqSyncIfTimingGnss2AlarmClr: CHASSIS [199](#)
 tmnxEqSyncIfTimingGnss2Quality: CHASSIS [200](#)
 tmnxEqSyncIfTimingGnssAlarm: CHASSIS [201](#)
 tmnxEqSyncIfTimingGnssAlarmClr: CHASSIS [201](#)
 tmnxEqSyncIfTimingGnssQuality: CHASSIS [202](#)
 tmnxEqSyncIfTimingHoldover: CHASSIS [202](#)
 tmnxEqSyncIfTimingHoldoverClear: CHASSIS [203](#)
 tmnxEqSyncIfTimingPTPAlarm: CHASSIS [204](#)
 tmnxEqSyncIfTimingPTPAlarmClr: CHASSIS [204](#)
 tmnxEqSyncIfTimingPTPQuality: CHASSIS [205](#)
 tmnxEqSyncIfTimingRef1Alarm: CHASSIS [206](#)
 tmnxEqSyncIfTimingRef1AlarmClear: CHASSIS [206](#)
 tmnxEqSyncIfTimingRef1Quality: CHASSIS [207](#)
 tmnxEqSyncIfTimingRef2Alarm: CHASSIS [208](#)
 tmnxEqSyncIfTimingRef2AlarmClear: CHASSIS [208](#)
 tmnxEqSyncIfTimingRef2Quality: CHASSIS [209](#)
 tmnxEqSyncIfTimingRefSwitch: CHASSIS [210](#)
 tmnxEqSyncIfTimingSyncE2Alarm: CHASSIS [210](#)
 tmnxEqSyncIfTimingSyncE2AlarmClr: CHASSIS [211](#)
 tmnxEqSyncIfTimingSyncE2Quality: CHASSIS [211](#)
 tmnxEqSyncIfTimingSyncEAlarm: CHASSIS [212](#)
 tmnxEqSyncIfTimingSyncEAlarmClr: CHASSIS [213](#)
 tmnxEqSyncIfTimingSyncEQuality: CHASSIS [213](#)
 tmnxEqSyncIfTimingSystemQuality: CHASSIS [214](#)
 tmnxEqWrongCard: CHASSIS [215](#)
 tmnxEsaCleared: CHASSIS [216](#)
 tmnxEsaConnected: CHASSIS [216](#)
 tmnxEsaDisconnected: CHASSIS [217](#)
 tmnxEsaDiscovered: CHASSIS [217](#)
 tmnxEsaFailure: CHASSIS [218](#)
 tmnxEsaFirmwareUpgradeDone: CHASSIS [219](#)
 tmnxEsaFirmwareUpgradeFailed: CHASSIS [219](#)
 tmnxEsaFirmwareUpgradeInProgress: CHASSIS [220](#)
 tmnxEsaFirmwareUpgradeStarted: CHASSIS [221](#)
 tmnxEsaHwFanBankFailRedun: CHASSIS [221](#)
 tmnxEsaHwFanBankFailRedunClr: CHASSIS [222](#)
 tmnxEsaHwFanBankNonRedun: CHASSIS [222](#)
 tmnxEsaHwFanBankNonRedunClr: CHASSIS [223](#)
 tmnxEsaHwFanStatusDegraded: CHASSIS [224](#)
 tmnxEsaHwFanStatusDegradedClr: CHASSIS [224](#)
 tmnxEsaHwFanStatusFailed: CHASSIS [225](#)
 tmnxEsaHwFanStatusFailedClr: CHASSIS [225](#)
 tmnxEsaHwPwrSup1Degraded: CHASSIS [226](#)
 tmnxEsaHwPwrSup1DegradedClr: CHASSIS [227](#)
 tmnxEsaHwPwrSup1Failed: CHASSIS [227](#)
 tmnxEsaHwPwrSup1FailedClr: CHASSIS [228](#)
 tmnxEsaHwPwrSup2Degraded: CHASSIS [228](#)
 tmnxEsaHwPwrSup2DegradedClr: CHASSIS [229](#)
 tmnxEsaHwPwrSup2Failed: CHASSIS [230](#)
 tmnxEsaHwPwrSup2FailedClr: CHASSIS [230](#)
 tmnxEsaHwPwrSupBankFailRedun: CHASSIS [231](#)
 tmnxEsaHwPwrSupBankFailRedunClr: CHASSIS [231](#)
 tmnxEsaHwPwrSupBankNonRedun: CHASSIS [232](#)
 tmnxEsaHwPwrSupBankNonRedunClr: CHASSIS [233](#)
 tmnxEsaHwPwrSupMismatch: CHASSIS [233](#)
 tmnxEsaHwPwrSupMismatchClr: CHASSIS [234](#)
 tmnxEsaHwStatusCritical: CHASSIS [234](#)
 tmnxEsaHwStatusCriticalClr: CHASSIS [235](#)
 tmnxEsaHwStatusDegraded: CHASSIS [236](#)
 tmnxEsaHwStatusDegradedClr: CHASSIS [236](#)
 tmnxEsaHwTemperatureDegraded: CHASSIS [237](#)
 tmnxEsaHwTemperatureDegradedClr: CHASSIS [237](#)
 tmnxEsaHwTemperatureFailed: CHASSIS [238](#)
 tmnxEsaHwTemperatureFailedClr: CHASSIS [239](#)
 tmnxEsaStolenTimeDetected: CHASSIS [239](#)
 tmnxEsaVmBooted: CHASSIS [240](#)
 tmnxEsaVmCleared: CHASSIS [241](#)
 tmnxEsaVmCreated: CHASSIS [241](#)
 tmnxEsaVmFailure: CHASSIS [242](#)
 tmnxEsaVmRemoved: CHASSIS [242](#)
 tmnxEthRingApsPrvsNClearAlarm: ERING [379](#)
 tmnxEthRingApsPrvsNRaiseAlarm: ERING [379](#)
 tmnxEthRingPathFwdStateChange: ERING [380](#)
 tmnxEthTunnelApsCfgClearAlarm: ETH_TUNNEL [390](#)
 tmnxEthTunnelApsCfgRaiseAlarm: ETH_TUNNEL [390](#)
 tmnxEthTunnelApsNoRspClearAlarm: ETH_TUNNEL [391](#)
 tmnxEthTunnelApsNoRspRaiseAlarm: ETH_TUNNEL [392](#)
 tmnxEthTunnelApsPrvsNClearAlarm: ETH_TUNNEL [392](#)

tmnxEthTunnelApsPrvsrnRaiseAlarm: ETH_TUNNEL 393
 tmnxEthTunnelApsSwitchoverAlarm: ETH_TUNNEL 394
 tmnxExtStandbyCpmReboot: CHASSIS 243
 tmnxExtStandbyCpmRebootFail: CHASSIS 244
 tmnxFileCopied: SECURITY 982
 tmnxFileDeleted: SECURITY 982
 tmnxFileMoved: SECURITY 983
 tmnxFileUnzip: SECURITY 984
 tmnxFPRResourcePolicyModified: CHASSIS 244
 tmnxFPRResourcePolicyModifiedClr: CHASSIS 245
 tmnxFPRResOversubscribed: CHASSIS 246
 tmnxFPRResOversubscribedCleared: CHASSIS 246
 tmnxFtpClientFailure: SYSTEM 1237
 tmnxGnssAcquiredFix: CHASSIS 247
 tmnxGnssAcquiringFix: CHASSIS 248
 tmnxHwAggShpSchedEventOvflw: CHASSIS 248
 tmnxHwAggShpSchedEventOvflwClr: CHASSIS 249
 tmnxHwAggShpSchedOperColorAmber: PORT 850
 tmnxHwAggShpSchedOperColorGreen: PORT 851
 tmnxHwAggShpSchedOperColorRed: PORT 851
 tmnxInterChassisCommsDown: CHASSIS 250
 tmnxInterChassisCommsUp: CHASSIS 250
 tmnxlomEventOverflow: CHASSIS 251
 tmnxlomEventOverflowClr: CHASSIS 252
 tmnxlomResExhausted: CHASSIS 252
 tmnxlomResHighLimitReached: CHASSIS 253
 tmnxlomResStateClr: CHASSIS 254
 tmnxlomRsrcEventOverflow: CHASSIS 254
 tmnxlomRsrcEventOverflowClr: CHASSIS 255
 tmnxlomRsrcOwnerOversubscrbdClr: CHASSIS 256
 tmnxlomRsrcOwnerOversubscribed: CHASSIS 257
 tmnxlomRsrcUsageExhausted: CHASSIS 257
 tmnxlomRsrcUsageHighLimitReached: CHASSIS 258
 tmnxlomRsrcUsageRecovered: CHASSIS 259
 tmnxIPMacCpmFilterOverload: CHASSIS 260
 tmnxIPMacCpmFilterOverloadClear: CHASSIS 260
 tmnxIPMacFilterEgrNearFull: CHASSIS 261
 tmnxIPMacFilterEgrNearFullClear: CHASSIS 262
 tmnxIPMacFilterEgrOverload: CHASSIS 262
 tmnxIPMacFilterEgrOverloadClear: CHASSIS 263
 tmnxIPMacFilterIngNearFull: CHASSIS 264
 tmnxIPMacFilterIngNearFullClear: CHASSIS 264
 tmnxIPMacFilterIngOverload: CHASSIS 265
 tmnxIPMacFilterIngOverloadClear: CHASSIS 266
 tmnxIPMacQosIngOverload: CHASSIS 266
 tmnxIPMacQosIngOverloadClear: CHASSIS 267
 tmnxIPQosEgrOverload: CHASSIS 268
 tmnxIPQosEgrOverloadClear: CHASSIS 269
 tmnxIPsecGWOperStateChange: IPSEC 447
 tmnxIPsecIslaGrpActiveIslaChgd: CHASSIS 269
 tmnxIPsecIslaGrpTnlHighWMark: CHASSIS 270
 tmnxIPsecIslaGrpTnlLowWMark: CHASSIS 271
 tmnxIPsecIslaGrpTnlMax: CHASSIS 271
 tmnxIPsecIslaGrpUnableToSwitch: CHASSIS 272
 tmnxIPsecTunnelOperStateChange: IPSEC 448
 tmnxIpTunnelOperRemIpChg: SVCMMGR 1169
 tmnxIpTunnelOperStateChange: SVCMMGR 1170
 tmnxIPv6CpmFilterOverload: CHASSIS 272
 tmnxIPv6CpmFilterOverloadClear: CHASSIS 273
 tmnxIPv6FilterEgrNearFull: CHASSIS 274
 tmnxIPv6FilterEgrNearFullClear: CHASSIS 274
 tmnxIPv6FilterEgrOverload: CHASSIS 275
 tmnxIPv6FilterEgrOverloadClear: CHASSIS 276
 tmnxIPv6FilterIngNearFull: CHASSIS 276
 tmnxIPv6FilterIngNearFullClear: CHASSIS 277
 tmnxIPv6FilterIngOverload: CHASSIS 278
 tmnxIPv6FilterIngOverloadClear: CHASSIS 278
 tmnxIPv6QosEgrOverload: CHASSIS 279
 tmnxIPv6QosEgrOverloadClear: CHASSIS 280
 tmnxIPv6QosIngOverload: CHASSIS 281
 tmnxIPv6QosIngOverloadClear: CHASSIS 281
 tmnxIsisAdjacencyChange: ISIS 452
 tmnxIsisAdjBfdSessionSetupFail: ISIS 452
 tmnxIsisAdjRestartStatusChange: ISIS 453
 tmnxIsisAreaMismatch: ISIS 454
 tmnxIsisAuthFail: ISIS 454
 tmnxIsisAutTypeFail: ISIS 455
 tmnxIsisCirCldExhausted: ISIS 456
 tmnxIsisCircMtuTooLow: ISIS 457
 tmnxIsisCorruptedLSPDetected: ISIS 457
 tmnxIsisCorruptRemainingLifetime: ISIS 458
 tmnxIsisDatabaseOverload: ISIS 459
 tmnxIsisExportLimitReached: ISIS 459
 tmnxIsisExportLimitWarning: ISIS 460
 tmnxIsisFailureDisabled: ISIS 461
 tmnxIsisFaOperParticipationDown: ISIS 461
 tmnxIsisIDLenMismatch: ISIS 462
 tmnxIsisLdpSyncExit: ISIS 463
 tmnxIsisLdpSyncTimerStarted: ISIS 464
 tmnxIsisLSPPurge: ISIS 464
 tmnxIsisLSPTooLargeToPropagate: ISIS 465
 tmnxIsisManualAddressDrops: ISIS 466
 tmnxIsisMaxAreaAdrsMismatch: ISIS 466
 tmnxIsisMaxSeqExceedAttempt: ISIS 467
 tmnxIsisOrigLSPBufSizeMismatch: ISIS 468
 tmnxIsisOwnLSPPurge: ISIS 469
 tmnxIsisPfxLimitOverloadWarning: ISIS 469
 tmnxIsisProtoSuppMismatch: ISIS 470
 tmnxIsisRejectedAdjacency: ISIS 471
 tmnxIsisRejectedAdjacencySet: ISIS 472
 tmnxIsisRejectedAdjacencySid: ISIS 472
 tmnxIsisRejectedEndXSid: ISIS 473
 tmnxIsisRejectedPgId: ISIS 474
 tmnxIsisRoutesExpLmtDropped: ISIS 474
 tmnxIsisSequenceNumberSkip: ISIS 475
 tmnxIsisSidError: ISIS 476
 tmnxIsisSidNotInLabelRange: ISIS 476
 tmnxIsisSidStatsIndexAlloc: ISIS 477
 tmnxIsisSrgbBadLabelRange: ISIS 478
 tmnxIsisSrv6LocError: ISIS 479
 tmnxIsisSrv6StaticSidIfTypeError: ISIS 479
 tmnxIsisVersionSkew: ISIS 480
 tmnxIxrResourceExhausted: CHASSIS 282
 tmnxIxrResourceExhaustedByOwner: CHASSIS 283

tmnxIxrResourceHighUsage: CHASSIS [283](#)
 tmnxIxrResourceHighUsageByOwner: CHASSIS [284](#)
 tmnxIxrResourceRecovered: CHASSIS [285](#)
 tmnxIxrResourceRecoveredByOwner: CHASSIS [285](#)
 tmnxKeyChainAuthFailure: SECURITY [984](#)
 tmnxL2tpApFailure: L2TP [484](#)
 tmnxL2tpIlsaMdaVRtrStateChange: L2TP [484](#)
 tmnxL2tpLnsPppNcpFailure: L2TP [485](#)
 tmnxL2tpLnsSePppSessionFailure: L2TP [486](#)
 tmnxL2tpPeerUnreachable: L2TP [486](#)
 tmnxL2tpTunnelBlacklisted: L2TP [487](#)
 tmnxL2tpTunnelSelBlacklistFull: L2TP [488](#)
 tmnxL2tpVappVRtrStateChange: L2TP [488](#)
 tmnxLagBfdMemStateChanged: LAG [495](#)
 tmnxLastSystemRebootAdmin: SYSTEM [1238](#)
 tmnxLdapOperStateChange: LDAP [496](#)
 tmnxLdapServerOperStateChange: LDAP [496](#)
 tmnxLldpRemEntryPeerAdded: LLDP [561](#)
 tmnxLldpRemEntryPeerRemoved: LLDP [562](#)
 tmnxLldpRemEntryPeerUpdated: LLDP [563](#)
 tmnxLldpRemManAddrEntryAdded: LLDP [563](#)
 tmnxLldpRemManAddrEntryRemoved: LLDP [564](#)
 tmnxLogAccountingDataLoss: LOGGER [570](#)
 tmnxLogAdminLocFailed: LOGGER [570](#)
 tmnxLogBackupLocFailed: LOGGER [571](#)
 tmnxLogEventOverrun: LOGGER [572](#)
 tmnxLogEventThrottled: LOGGER [573](#)
 tmnxLogFileDeleted: LOGGER [573](#)
 tmnxLogFileRollover: LOGGER [574](#)
 tmnxLogOnlyEventOverrun: LOGGER [575](#)
 tmnxLogOnlyEventThrottled: LOGGER [575](#)
 tmnxLogSpaceContention: LOGGER [576](#)
 tmnxLogTraceError: LOGGER [577](#)
 tmnxLudbDhcpGroupIfTooLong: DHCP [362](#)
 tmnxLudbPppoeGroupIfTooLong: DHCP [363](#)
 tmnxMacsecCaCreate: MACSEC [581](#)
 tmnxMacsecConfiguredPortCA: MACSEC [581](#)
 tmnxMacsecDisabledPort: MACSEC [582](#)
 tmnxMacsecDpReplayAttempt: MACSEC [583](#)
 tmnxMacsecEnabledPort: MACSEC [583](#)
 tmnxMacsecMaxPeerLimitCleared: MACSEC [584](#)
 tmnxMacsecMaxPeerLimitExceeded: MACSEC [584](#)
 tmnxMacsecMkaReplayAttemptDisc: MACSEC [585](#)
 tmnxMacsecSakCreate: MACSEC [586](#)
 tmnxMacsecSakDelete: MACSEC [586](#)
 tmnxMacsecSakInstalledRx: MACSEC [587](#)
 tmnxMacsecSakInstalledTx: MACSEC [588](#)
 tmnxMacsecUnconfiguredPortCA: MACSEC [588](#)
 tmnxMCEPSessionPsvModeDisabled: MC_REDUNDANCY [596](#)
 tmnxMCEPSessionPsvModeEnabled: MC_REDUNDANCY [597](#)
 tmnxMcLagInfoLagChanged: MC_REDUNDANCY [598](#)
 tmnxMcOmcrClientNumEntriesHigh: MC_REDUNDANCY [598](#)
 tmnxMcOmcrStatFailedChanged: MC_REDUNDANCY [599](#)
 tmnxMcPathAvailBwLimitCleared: MCPATH [624](#)
 tmnxMcPathAvailBwLimitExceeded: MCPATH [624](#)
 tmnxMcPathSrcGrpBlackHole: MCPATH [625](#)
 tmnxMcPathSrcGrpBlackHoleCleared: MCPATH [626](#)
 tmnxMcPeerEPBfdSessionClose: MC_REDUNDANCY [600](#)
 tmnxMcPeerEPBfdSessionDown: MC_REDUNDANCY [601](#)
 tmnxMcPeerEPBfdSessionOpen: MC_REDUNDANCY [602](#)
 tmnxMcPeerEPBfdSessionUp: MC_REDUNDANCY [602](#)
 tmnxMcPeerEPOperDown: MC_REDUNDANCY [603](#)
 tmnxMcPeerEPOperUp: MC_REDUNDANCY [603](#)
 tmnxMcPeerRingsOperStateChanged: MC_REDUNDANCY [604](#)
 tmnxMcPeerSyncStatusChanged: MC_REDUNDANCY [605](#)
 tmnxMcRedundancyMismatchDetected: MC_REDUNDANCY [606](#)
 tmnxMcRedundancyMismatchResolved: MC_REDUNDANCY [606](#)
 tmnxMcRedundancyPeerStateChanged: MC_REDUNDANCY [607](#)
 tmnxMcRingInbCtrlOperStateChgd: MC_REDUNDANCY [607](#)
 tmnxMcRingNodeLocOperStateChgd: MC_REDUNDANCY [608](#)
 tmnxMcRingOperStateChanged: MC_REDUNDANCY [609](#)
 tmnxMcSyncClientAlarmCleared: MC_REDUNDANCY [610](#)
 tmnxMcSyncClientAlarmRaised: MC_REDUNDANCY [611](#)
 tmnxMcSyncClockSkewCleared: MC_REDUNDANCY [612](#)
 tmnxMcSyncClockSkewRaised: MC_REDUNDANCY [612](#)
 tmnxMD5AuthFailure: SECURITY [985](#)
 tmnxMDAIsaTunnelGroupChange: CHASSIS [286](#)
 tmnxMkaOperStateChanged: MACSEC [589](#)
 tmnxMkaPskRollover: MACSEC [590](#)
 tmnxMkaSessionEnded: MACSEC [590](#)
 tmnxMkaSessionEstablished: MACSEC [591](#)
 tmnxMlpppBundleIndicatorsChange: PPPOE [867](#)
 tmnxModuleMallocFailed: SYSTEM [1239](#)
 tmnxMplsResourceExhausted: MPLS [662](#)
 tmnxMplsResourceHighUsage: MPLS [663](#)
 tmnxMplsResourceRecovered: MPLS [664](#)
 tmnxMsdpNgActSrcLimExcd: MSDP [689](#)
 tmnxMsdpNgGroupSrcActMsgsExcd: MSDP [689](#)
 tmnxMsdpNgPeerActSrcLimExcd: MSDP [690](#)
 tmnxMsdpNgRPFFailure: MSDP [691](#)
 tmnxMsdpNgSourceSrcActMsgsExcd: MSDP [691](#)
 tmnxNatDetAddrMapOperStateChngd: NAT [693](#)
 tmnxNatDetMap2OperStateChanged: NAT [693](#)
 tmnxNatDetPfxMapOperStateChanged: NAT [694](#)
 tmnxNatDetPlycChanged: NAT [695](#)
 tmnxNatDynamicConfigMismatch: NAT [695](#)
 tmnxNatFwd2EntryAdded: NAT [696](#)
 tmnxNatFwd2OperStateChanged: NAT [697](#)
 tmnxNatInAddrPrefixBlksFree: NAT [698](#)
 tmnxNatIlsaGrplsDegraded: NAT [699](#)
 tmnxNatIlsaGrpOperStateChanged: NAT [700](#)
 tmnxNatIlsaMemberSessionUsageHigh: NAT [700](#)
 tmnxNatL2AwSublcmpPortUsageHigh: NAT [701](#)
 tmnxNatL2AwSubSessionUsageHigh: NAT [701](#)
 tmnxNatL2AwSubTcpPortUsageHigh: NAT [702](#)

tmnxNatL2AwSubUdpPortUsageHigh: NAT 703
 tmnxNatLsnSubBlksFree: NAT 703
 tmnxNatLsnSubLcmpPortUsgHigh: NAT 704
 tmnxNatLsnSubSessionUsgHigh: NAT 705
 tmnxNatLsnSubTcpPortUsgHigh: NAT 706
 tmnxNatLsnSubUdpPortUsgHigh: NAT 706
 tmnxNatMapRuleChange: NAT 707
 tmnxNatMaxNbrSubsOrHostsExceeded: NAT 708
 tmnxNatMdaActive: NAT 709
 tmnxNatMdaDetectsLoadSharingErr: NAT 709
 tmnxNatNbrSubsOrHostsBelowThrsh: NAT 710
 tmnxNatPcpSrvStateChanged: NAT 711
 tmnxNatPIAddrFree: NAT 711
 tmnxNatPIBlockAllocationL2Aw: NAT 712
 tmnxNatPIBlockAllocationLsn: NAT 713
 tmnxNatPIL2AwBlockUsageHigh: NAT 714
 tmnxNatPIL2AwMembrBlockUsageHigh: NAT 715
 tmnxNatPILsnMemberBlockUsageHigh: NAT 716
 tmnxNatPILsnMemberPortUsageHigh: NAT 716
 tmnxNatPILsnRedActiveChanged: NAT 717
 tmnxNatPIMemberExtBlockUsageHigh: NAT 718
 tmnxNatResourceProblemCause: NAT 719
 tmnxNatResourceProblemDetected: NAT 719
 tmnxNatVappActive: NAT 720
 tmnxNatVappDetectsLoadSharingErr: NAT 721
 tmnxNatVrtrOutDnatOnlyRoutesHigh: NAT 721
 tmnxNetconfNotifyOverrun: LOGGER 577
 tmnxNewCistRegionalRootBridge: STP 1053
 tmnxNewMstiRegionalRootBridge: STP 1054
 tmnxNtpAuthMismatch: NTP 723
 tmnxNtpNoServersAvail: NTP 723
 tmnxNtpOperChange: NTP 724
 tmnxNtpServerChange: NTP 725
 tmnxNtpServersAvail: NTP 725
 tmnxOamDiagTestCompleted: OAM 729
 tmnxOamLdpTtraceAutoDiscState: OAM 730
 tmnxOamLdpTtraceFecDisStatus: OAM 730
 tmnxOamLdpTtraceFecPFailUpdate: OAM 731
 tmnxOamLdpTtraceFecProbeState: OAM 732
 tmnxOamPingProbeFailedV3: OAM 732
 tmnxOamPingTestCompletedV3: OAM 733
 tmnxOamPingTestFailedV3: OAM 734
 tmnxOamPmThrClear: OAM 734
 tmnxOamPmThrRaise: OAM 735
 tmnxOamSaaThreshold: OAM 737
 tmnxOamSathSvcStrmCompleted: OAM 737
 tmnxOamSathSvcTestCompleted: OAM 738
 tmnxOamTrPathChange: OAM 739
 tmnxOamTrTestCompleted: OAM 739
 tmnxOamTrTestFailed: OAM 740
 tmnxOFFlowEntryInsertFailed: OPEN_FLOW 746
 tmnxOspfAdjBfdSessionSetupFail: OSPF 747
 tmnxOspfAreaMaxAgeLsa: OSPF 747
 tmnxOspfAreaOriginateLsa: OSPF 748
 tmnxOspfAsMaxAgeLsa: OSPF 749
 tmnxOspfAsOriginateLsa: OSPF 749
 tmnxOspfDynHostnameDuplicate: OSPF 750
 tmnxOspfDynHostnameInconsistent: OSPF 750
 tmnxOspfExportLimitReached: OSPF 751
 tmnxOspfExportLimitWarning: OSPF 752
 tmnxOspfFailureDisabled: OSPF 752
 tmnxOspfFaOperParticipationDown: OSPF 753
 tmnxOspfLsdbApproachingOverflow: OSPF 754
 tmnxOspfLsdbOverflow: OSPF 754
 tmnxOspfNgIfAuthFailure: OSPF 755
 tmnxOspfNgIfConfigError: OSPF 756
 tmnxOspfNgIfRxBadPacket: OSPF 756
 tmnxOspfNgIfStateChange: OSPF 757
 tmnxOspfNgLdpSyncExit: OSPF 758
 tmnxOspfNgLdpSyncTimerStarted: OSPF 758
 tmnxOspfNgLinkMaxAgeLsa: OSPF 759
 tmnxOspfNgLinkOriginateLsa: OSPF 759
 tmnxOspfNgNbrRestartHlprStsChg: OSPF 760
 tmnxOspfNgNbrStateChange: OSPF 761
 tmnxOspfNgNbrStrictBfdBlocked: OSPF 762
 tmnxOspfNssaTranslatorStatusChg: OSPF 762
 tmnxOspfOverloadEntered: OSPF 763
 tmnxOspfOverloadExited: OSPF 764
 tmnxOspfOverloadWarning: OSPF 764
 tmnxOspfRejectedAdjacencySet: OSPF 765
 tmnxOspfRejectedAdjacencySid: OSPF 765
 tmnxOspfRestartStatusChange: OSPF 766
 tmnxOspfRoutesExpLmtDropped: OSPF 767
 tmnxOspfShamIfAuthFailure: OSPF 767
 tmnxOspfShamIfConfigError: OSPF 768
 tmnxOspfShamIfRxBadPacket: OSPF 769
 tmnxOspfShamIfStateChange: OSPF 770
 tmnxOspfShamNbrRestartHlprStsChg: OSPF 770
 tmnxOspfShamNbrStateChange: OSPF 771
 tmnxOspfSidStatsIndexAlloc: OSPF 772
 tmnxOspfSpfRunsRestarted: OSPF 773
 tmnxOspfSpfRunsStopped: OSPF 773
 tmnxOspfSrgbBadLabelRange: OSPF 774
 tmnxOspfSrSidError: OSPF 774
 tmnxOspfSrSidNotInLabelRange: OSPF 775
 tmnxOspfVirtIfAuthFailure: OSPF 776
 tmnxOspfVirtIfConfigError: OSPF 777
 tmnxOspfVirtIfRxBadPacket: OSPF 777
 tmnxOspfVirtIfStateChange: OSPF 778
 tmnxOspfVirtNbrRestartHlprStsChg: OSPF 779
 tmnxOspfVirtNbrStateChange: OSPF 779
 tmnxPasswordHashingChanged: SECURITY 986
 tmnxPcapBufferFull: PCAP 781
 tmnxPcapBufferReadWriteFailure: PCAP 781
 tmnxPcapFileError: PCAP 782
 tmnxPcapSoftwareFailure: PCAP 783
 tmnxPcepPccPeerStateChange: PCEP 784
 tmnxPeBootloaderVersionMismatch: CHASSIS 287
 tmnxPeBootromVersionMismatch: CHASSIS 287
 tmnxPeFirmwareVersionWarning: CHASSIS 288
 tmnxPeFPGAVersionMismatch: CHASSIS 289
 tmnxPeKernelVersionMismatch: CHASSIS 289
 tmnxPeSoftwareLoadFailed: CHASSIS 290
 tmnxPeSoftwareVersionMismatch: CHASSIS 291

tmnxPfcPAssocPathMgmtStateChgd: SVC MGR 1171
 tmnxPfcPInvalidId: PFCP 785
 tmnxPfcPNoSecondaryInterface: PFCP 785
 tmnxPfcPNoSuchCallTraceProfile: PFCP 786
 tmnxPhysChassisFilterDoorClosed: CHASSIS 291
 tmnxPhysChassisFilterDoorOpen: CHASSIS 292
 tmnxPhysChassisPCMinputFeed: CHASSIS 293
 tmnxPhysChassisPCMinputFeedClr: CHASSIS 293
 tmnxPhysChassisPMinputFeed: CHASSIS 294
 tmnxPhysChassisPMinputFeedClr: CHASSIS 294
 tmnxPhysChassisPMOutFail: CHASSIS 295
 tmnxPhysChassisPMOutFailClr: CHASSIS 296
 tmnxPhysChassisPMOverTemp: CHASSIS 296
 tmnxPhysChassisPMOverTempClr: CHASSIS 297
 tmnxPhysChassPwrSupInputFeed: CHASSIS 297
 tmnxPhysChassPwrSupInputFeedClr: CHASSIS 298
 tmnxPhysChassPwrSupPemACRect: CHASSIS 299
 tmnxPhysChassPwrSupPemACRectClr: CHASSIS 299
 tmnxPhysChassPwrSupWrgFanDir: CHASSIS 300
 tmnxPhysChassPwrSupWrgFanDirClr: CHASSIS 301
 tmnxPimSnpGlfMaxNbrReached: PIM_SNOOPING 802
 tmnxPimSnpGlfNeighborLoss: PIM_SNOOPING 802
 tmnxPimSnpGlfNeighborUp: PIM_SNOOPING 803
 tmnxPimSnpGMaxNbrReached: PIM_SNOOPING 803
 tmnxPimSnpGSGLimitExceeded: PIM_SNOOPING 804
 tmnxPimSnpGSnoopModeChanged: PIM_SNOOPING 805
 tmnxPipStpExcepCondStateChng: STP 1055
 tmnxPkiCAProfActnStatusChg: SECURITY 987
 tmnxPkiCAProfCrlUpdAllUrIsFail: SECURITY 987
 tmnxPkiCAProfCrlUpdateStart: SECURITY 988
 tmnxPkiCAProfCrlUpdateSuccess: SECURITY 989
 tmnxPkiCAProfCrlUpdateUrlFail: SECURITY 989
 tmnxPkiCAProfCrlUpdLargPreUpdTm: SECURITY 990
 tmnxPkiCAProfCrlUpdNoNxtUpdTime: SECURITY 991
 tmnxPkiCAProfRevokeChkWarning: SECURITY 992
 tmnxPkiCertAfterExpWarning: SECURITY 993
 tmnxPkiCertBeforeExpWarning: SECURITY 993
 tmnxPkiCertChainCompareCaNoMatch: SECURITY 994
 tmnxPkiCertExpWarningCleared: SECURITY 995
 tmnxPkiCertNotYetValid: SECURITY 995
 tmnxPkiCertUpdUpdateFailed: SECURITY 996
 tmnxPkiCertUpdUpdateFinished: SECURITY 997
 tmnxPkiCertUpdUpdateStarted: SECURITY 997
 tmnxPkiCertVerificationFailed: SECURITY 998
 tmnxPkiCRLAfterExpWarning: SECURITY 998
 tmnxPkiCRLBeforeExpWarning: SECURITY 999
 tmnxPkiCRLExpWarningCleared: SECURITY 1000
 tmnxPkiCRLNotYetValid: SECURITY 1000
 tmnxPkiFileReadFailed: SECURITY 1001
 tmnxPkiFileWriteFailed: SECURITY 1002
 tmnxPlyAcctPcrPoolExcResource: CHASSIS 301
 tmnxPlyAcctPcrPoolLowResource: CHASSIS 302
 tmnxPlyAcctStatsEventOvrflw: CHASSIS 303
 tmnxPlyAcctStatsEventOvrflwClr: CHASSIS 303
 tmnxPlyAcctStatsPoolExcResource: CHASSIS 304
 tmnxPlyAcctStatsPoolLowResource: CHASSIS 305
 tmnxPortAUIReset: PORT 852
 tmnxPortEtherLoopbackStarted: PORT 853
 tmnxPortEtherLoopbackStopped: PORT 853
 tmnxPortGnssStatusChange: PORT 854
 tmnxPortUnsupportedFunction: PORT 855
 tmnxPowerShelfCommsDown: CHASSIS 306
 tmnxPowerShelfCommsUp: CHASSIS 306
 tmnxPowerShelfInputPwrModeSwitch: CHASSIS 307
 tmnxPowerShelfOutputStatusDown: CHASSIS 307
 tmnxPowerShelfOutputStatusSwitch: CHASSIS 308
 tmnxPowerShelfOutputStatusUp: CHASSIS 309
 tmnxPowerSupplyFanFailed: CHASSIS 309
 tmnxPowerSupplyFanFailedClear: CHASSIS 310
 tmnxPppoeClientEchoTimeout: PPPOE_CLNT 873
 tmnxPppoeClientNcpFailure: PPPOE_CLNT 873
 tmnxPppoeClientSetupFailure: PPPOE_CLNT 874
 tmnxPppoeLacFragFailed: PPPOE 867
 tmnxPppoeLacSteeringActive: PPPOE 868
 tmnxPppoeLacSteeringFailed: PPPOE 869
 tmnxPppoeLacSteeringStopped: PPPOE 869
 tmnxPppoeMaxSessionsOvrExceeded: PPPOE 870
 tmnxPppoeNcpFailure: PPPOE 871
 tmnxPppoeSessionFailure: PPPOE 871
 tmnxPtpCardNotSupported: PTP 875
 tmnxPtpCardNotSupportedClear: PTP 875
 tmnxPtpClockRecoveryStateChange: PTP 876
 tmnxPtpDynamicChange: PTP 877
 tmnxPtpMasterClockChangedEvent: PTP 877
 tmnxPtpOutOfResources: PTP 878
 tmnxPtpOutOfResourcesClear: PTP 879
 tmnxPtpPeerNoRxTimestamping: PTP 879
 tmnxPtpPeerNoRxTimestampingClear: PTP 880
 tmnxPtpPeerNoTxTimestamping: PTP 881
 tmnxPtpPeerNoTxTimestampingClear: PTP 882
 tmnxPtpPortNoTimestamping: PTP 882
 tmnxPtpPortPtsfUnusable: PTP 883
 tmnxPtpRequiresSystemReboot: PTP 884
 tmnxPtpRequiresSystemRebootClear: PTP 884
 tmnxPtpTimeRecoveryStateChange: PTP 885
 tmnxPythonInterpreterRestarted: PYTHON 887
 tmnxRadAcctOnOngoing: RADIUS 888
 tmnxRadRouteDownloadFailed: RADIUS 888
 tmnxRadSrvPlySrvOperStateCh: RADIUS 889
 tmnxRedCpmActive: SYSTEM 1239
 tmnxRedPrimaryCPMFail: CHASSIS 311
 tmnxRedSingleCpm: SYSTEM 1240
 tmnxRedStandbyReady: SYSTEM 1241
 tmnxRedStandbySyncing: SYSTEM 1241
 tmnxRedStandbySyncLost: SYSTEM 1242
 tmnxRedSwitchover: SYSTEM 1242
 tmnxResvCbsPoolThreshAmber: PORT 855
 tmnxResvCbsPoolThreshGreen: PORT 856
 tmnxResvCbsPoolThreshRed: PORT 857
 tmnxResvPoolUseThreshExcd: PORT 857
 tmnxResvPoolUseThreshNotExcd: PORT 858
 tmnxRipNgAuthFailure: RIP_NG 897
 tmnxRipNgAuthTypeMismatch: RIP_NG 897
 tmnxRipNgUcastAddrNotUsed: RIP_NG 898

tmnxRipNgInstExpLmtReached: RIP_NG 899
 tmnxRipNgInstExpLmtWarning: RIP_NG 899
 tmnxRipNgInstRestarted: RIP_NG 900
 tmnxRipNgInstRtsExpLmtDropped: RIP_NG 901
 tmnxRipNgInstShuttingDown: RIP_NG 901
 tmnxRipNgPacketDiscarded: RIP_NG 902
 tmnxRipNgPeerBfdDown: RIP_NG 903
 tmnxRpkiNotifySession: RPKI 905
 tmnxRpkiStaleTimerExpiry: RPKI 905
 tmnxRS232ControlLeadSignalChg: PORT 859
 tmnxRS232SquelchResetIssued: PORT 859
 tmnxRS232SquelchStatusChange: PORT 860
 tmnxSapMRtCpeChkStatusChange: SVC_MGR 1171
 tmnxSapStpExcepCondStateChng: STP 1055
 tmnxSapStpExcepCondStateChng: SVC_MGR 1172
 tmnxSasAlarminput1StateChanged: CHASSIS 311
 tmnxSasAlarminput2StateChanged: CHASSIS 312
 tmnxSasAlarminput3StateChanged: CHASSIS 313
 tmnxSasAlarminput4StateChanged: CHASSIS 314
 tmnxSatelliteOperStateChange: SATELLITE 911
 tmnxSatLocalForwardSapStateChg: SATELLITE 911
 tmnxSatLocalForwardStateChg: SATELLITE 912
 tmnxSatSynclfTimHoldover: SATELLITE 913
 tmnxSatSynclfTimHoldoverClear: SATELLITE 914
 tmnxSatSynclfTimRef1Alarm: SATELLITE 914
 tmnxSatSynclfTimRef1AlarmClear: SATELLITE 915
 tmnxSatSynclfTimRef1Quality: SATELLITE 916
 tmnxSatSynclfTimRef2Alarm: SATELLITE 916
 tmnxSatSynclfTimRef2AlarmClear: SATELLITE 917
 tmnxSatSynclfTimRef2Quality: SATELLITE 917
 tmnxSatSynclfTimRefSwitch: SATELLITE 918
 tmnxSatSynclfTimSystemQuality: SATELLITE 919
 tmnxSdpBndStpExcepCondStateChng: STP 1056
 tmnxSecComputeCertChainFailure: SECURITY 1003
 tmnxSecNotifCmptedCertChnChngd: IPSEC 448
 tmnxSecNotifCmptedCertHashChngd: IPSEC 449
 tmnxSecNotifFileReloaded: SECURITY 1003
 tmnxSecNotifKeyChainExpired: SECURITY 1004
 tmnxSecNotifSendChnNotInCmptChn: IPSEC 450
 tmnxSecPwdHistoryFileLoadFailed: SECURITY 1004
 tmnxSecPwdHistoryFileWriteFailed: SECURITY 1005
 tmnxSecSignedSwCpmBootEvent: SECURITY 1006
 tmnxSecSignedSwImgValFail: SECURITY 1006
 tmnxSflowCpEntrySampling: SFLOW 1036
 tmnxSflowPacketTxFailure: SFLOW 1036
 tmnxSfmIcPortDDMClear: CHASSIS 314
 tmnxSfmIcPortDDMFailure: CHASSIS 315
 tmnxSfmIcPortDegraded: CHASSIS 316
 tmnxSfmIcPortDegradedClear: CHASSIS 316
 tmnxSfmIcPortDown: CHASSIS 317
 tmnxSfmIcPortSFFInserted: CHASSIS 318
 tmnxSfmIcPortSFFRemoved: CHASSIS 319
 tmnxSfmIcPortUp: CHASSIS 319
 tmnxSharedPoolUseThreshExcd: PORT 860
 tmnxSharedPoolUseThreshNotExcd: PORT 861
 tmnxSmLaunchStartFailed: SYSTEM 1243
 tmnxSnpdStateChange: SYSTEM 1244
 tmnxSntpOperChange: SYSTEM 1244
 tmnxSrMplsPfxSidFailure: SR_MPLS 1044
 tmnxSrMplsPfxSidFlexAlgoFailure: SR_MPLS 1044
 tmnxSrrpBecameBackup: MC_REDUNDANCY 613
 tmnxSrrpBfdIntfSessStateChgd: MC_REDUNDANCY 613
 tmnxSrrpDualMaster: MC_REDUNDANCY 614
 tmnxSrrpDuplicateSubIfAddress: MC_REDUNDANCY 615
 tmnxSrrpInstanceldMismatch: MC_REDUNDANCY 615
 tmnxSrrpOperDownInvalidMac: MC_REDUNDANCY 616
 tmnxSrrpOperDownInvalidMacClear: MC_REDUNDANCY 617
 tmnxSrrpPrivRetailMismatch: MC_REDUNDANCY 617
 tmnxSrrpRedIfMismatch: MC_REDUNDANCY 618
 tmnxSrrpSapMismatch: MC_REDUNDANCY 619
 tmnxSrrpSapTagMismatch: MC_REDUNDANCY 619
 tmnxSrrpSubnetMismatch: MC_REDUNDANCY 620
 tmnxSrrpSubnetMismatchCleared: MC_REDUNDANCY 621
 tmnxSrrpSystemIpNotSet: MC_REDUNDANCY 621
 tmnxSrrpTrapNewMaster: MC_REDUNDANCY 622
 tmnxSSHInvalidPacketLength: SECURITY 1007
 tmnxSSHListeningPortChanged: SECURITY 1008
 tmnxSSHListeningPortInUse: SECURITY 1009
 tmnxSSHListeningPortOccupied: SECURITY 1009
 tmnxSSHSessionFailed: SECURITY 1010
 tmnxSssiMismatch: SYSTEM 1245
 tmnxStateChange: LI 560
 tmnxStateChange: SECURITY 1011
 tmnxStateChange: SYSTEM 1246
 tmnxStdEventsReplayed: LOGGER 578
 tmnxStpMeshNotInMstRegion: STP 1056
 tmnxStpRootGuardViolation: STP 1057
 tmnxStpRootGuardViolation: SVC_MGR 1173
 tmnxSubAcctPclyFailure: SVC_MGR 1173
 tmnxSubAcctPclyRadSerOperStatChg: SVC_MGR 1174
 tmnxSubAuthPclyRadSerOperStatChg: SVC_MGR 1175
 tmnxSubBrgCreated: SVC_MGR 1175
 tmnxSubBrgCvInitFailed: SVC_MGR 1176
 tmnxSubBrgDeleted: SVC_MGR 1177
 tmnxSubBrgRadiusAuthError: SVC_MGR 1177
 tmnxSubBrgRadiusCoaError: SVC_MGR 1178
 tmnxSubBrgRadiusProxyAuthError: SVC_MGR 1179
 tmnxSubBrgRadiusUpdateIpoeSeFail: SVC_MGR 1179
 tmnxSubBrgSessionLimitReached: SVC_MGR 1180
 tmnxSubCupsUpIfCreationFailed: SVC_MGR 1181
 tmnxSubCupsUpSapCreationFailed: SVC_MGR 1182
 tmnxSubDhcpOverloadDetected: SVC_MGR 1182
 tmnxSubHostInconsistentAtmTdOvr: SVC_MGR 1183
 tmnxSubHostInfoConflict: SVC_MGR 1184
 tmnxSubHostLcktLimitReached: SVC_MGR 1184
 tmnxSubHostLcktSapLimitReached: SVC_MGR 1185
 tmnxSubInfoEgrAggRateLimitLowReq: SVC_MGR 1185
 tmnxSubIpoeInvalidCidRidChange: SVC_MGR 1186
 tmnxSubIpoeInvalidSessionKey: SVC_MGR 1187
 tmnxSubIpoeMigrHostDeleted: SVC_MGR 1187
 tmnxSubIpoePersistenceRecovery: SVC_MGR 1188
 tmnxSubIpoeSessionBrgNotAuth: SVC_MGR 1189
 tmnxSubIpoeSessionLimitReached: SVC_MGR 1189

tmnxSubIpoeWppRegistrationFailed: SVCMMGR 1190
 tmnxSubMcsRelatedProblem: SVCMMGR 1191
 tmnxSubMngdHostCreationFail: SVCMMGR 1191
 tmnxSubMngdHostOverride: SVCMMGR 1192
 tmnxSubPIBndFailed: SVCMMGR 1193
 tmnxSubPysrosExec: SVCMMGR 1193
 tmnxSubPysrosExecFail: SVCMMGR 1194
 tmnxSubRadiusCoaNatFwdFailed: SVCMMGR 1195
 tmnxSubRadSapCoAError: SVCMMGR 1195
 tmnxSubRadSapDisconnectError: SVCMMGR 1196
 tmnxSubRadSapSubAuthError: SVCMMGR 1197
 tmnxSubRadSdpBndCoAError: SVCMMGR 1197
 tmnxSubRadSdpBndDisconnectError: SVCMMGR 1198
 tmnxSubRadSdpBndSubAuthError: SVCMMGR 1199
 tmnxSubscriberCreated: SVCMMGR 1199
 tmnxSubscriberDeleted: SVCMMGR 1200
 tmnxSubscriberRenamed: SVCMMGR 1200
 tmnxSubSlaacOverride: SVCMMGR 1201
 tmnxSubSlaacSetupFailure: SVCMMGR 1202
 tmnxSubStatsResourceLimitReached: SVCMMGR 1202
 tmnxSubSVlanStatsReachedMaximum: SVCMMGR 1203
 tmnxSubSysChassMemoryUsageHi: SVCMMGR 1204
 tmnxSubUserCategoryError: SVCMMGR 1205
 tmnxSubUserCategoryOutOfCredit: SVCMMGR 1205
 tmnxSubUserCategoryRefreshCredit: SVCMMGR 1206
 tmnxSubVSubnetHostsDeleted: SVCMMGR 1207
 tmnxSvcNewRootSdpBind: STP 1058
 tmnxSvcSdpActiveProtocolChange: STP 1058
 tmnxSvcSdpBindEncapDot1d: STP 1059
 tmnxSvcSdpBindEncapPVST: STP 1059
 tmnxSvcSdpBindRcvdHigherBriPrio: STP 1060
 tmnxSvcSdpBindRcvdTCN: STP 1061
 tmnxSvcSysFdbTableHighUsgClr: SVCMMGR 1207
 tmnxSvcSysFdbTableHighUsgSet: SVCMMGR 1208
 tmnxSvcTopoChgSdpBindMajorState: STP 1061
 tmnxSvcTopoChgSdpBindState: STP 1062
 tmnxSynclfTimBITS2048khzUnsup: CHASSIS 320
 tmnxSynclfTimBITS2048khzUnsupClr: CHASSIS 321
 tmnxSysAppLicenseInsufficient: SECURITY 1011
 tmnxSysAppStats24HrsAvailable: SYSTEM 1246
 tmnxSysAppStatsWeekAvailable: SYSTEM 1247
 tmnxSysBaseMacAddressNotSet: SYSTEM 1248
 tmnxSysDyingGasp: SYSTEM 1248
 tmnxSysExecFinished: SYSTEM 1249
 tmnxSysExecStarted: SYSTEM 1250
 tmnxSysHttpRdrOutOfSeqLimitExc: SYSTEM 1251
 tmnxSysLicenseActivated: SECURITY 1012
 tmnxSysLicenseCleared: SECURITY 1013
 tmnxSysLicenseExpiresSoon: SECURITY 1013
 tmnxSysLicenseInvalid: SECURITY 1014
 tmnxSysLicenseUpdateRequired: SECURITY 1014
 tmnxSysLicenseValid: SECURITY 1015
 tmnxSysLicensingStateOk: SECURITY 1016
 tmnxSysLogTargetProblem: LOGGER 579
 tmnxSysMgmtlflLicfgNotEncrypted: SYSTEM 1252
 tmnxSysMgmtlflLicfgIncorrectFormat: SYSTEM 1252
 tmnxSysMgmtlflModeChangeComplete: SYSTEM 1253
 tmnxSysMgmtlflModeChangeFailure: SYSTEM 1254
 tmnxSysMgmtlflModeChangeStart: SYSTEM 1254
 tmnxSysNvsysFileError: SYSTEM 1255
 tmnxSysRollbackDeleteStarted: SYSTEM 1256
 tmnxSysRollbackFileDeleteStatus: SYSTEM 1256
 tmnxSysRollbackSaveStarted: SYSTEM 1257
 tmnxSysRollbackSaveStatusChange: SYSTEM 1258
 tmnxSysRollbackStarted: SYSTEM 1258
 tmnxSysRollbackStatusChange: SYSTEM 1259
 tmnxSysStandbyLicensingError: SECURITY 1016
 tmnxSysStandbyLicensingReady: SECURITY 1017
 tmnxSysSwDSValidationResult: SECURITY 1018
 tmnxSysSwFabFailRecAborted: SYSTEM 1260
 tmnxSysSwFabFailRecCompleted: SYSTEM 1260
 tmnxSysSwFabFailRecDetected: SYSTEM 1261
 tmnxSysSwFabFailRecStarted: SYSTEM 1262
 tmnxSystemPasswordChangedByAdmin: SECURITY 1018
 tmnxTelnetListeningPortChanged: SECURITY 1019
 tmnxTelnetListeningPortInUse: SECURITY 1020
 tmnxTelnetListeningPortOccupied: SECURITY 1020
 tmnxTestEvent: LOGGER 580
 tmnxTlsFailure: TLS 1264
 tmnxTlsInitiateSession: TLS 1264
 tmnxTlsTermination: TLS 1265
 tmnxTotalPoolUseThreshExcd: PORT 862
 tmnxTotalPoolUseThreshNotExcd: PORT 863
 tmnxTrapDropped: SYSTEM 1262
 tmnxTunnelGrpEsaVmActivity: CHASSIS 321
 tmnxTwampRflInactivityTimeout: OAM 740
 tmnxTwampSrvInactivityTimeout: OAM 741
 tmnxTwampSrvMaxConnsExceeded: OAM 742
 tmnxTwampSrvMaxSessExceeded: OAM 743
 tmnxTwampSrvPfxMaxConnsExceeded: OAM 743
 tmnxTwampSrvPfxMaxSessExceeded: OAM 744
 tmnxUserPasswordChangedByAdmin: SECURITY 1021
 tmnxUsrProfSessionLimitExceeded: SECURITY 1022
 tmnxVdoAdSpliceAbort: VIDEO 1287
 tmnxVdoClientSessionsLmtCleared: VIDEO 1287
 tmnxVdoClientSessionsLmtExceeded: VIDEO 1288
 tmnxVdoDuplicateSsrclId: VIDEO 1289
 tmnxVdoGrpSrcAnlyzrErrState: VIDEO 1289
 tmnxVdoGrpSrcAnlyzrStClear: VIDEO 1290
 tmnxVdoMdaFccBwLimitCleared: VIDEO 1291
 tmnxVdoMdaFccBwLimitExceeded: VIDEO 1291
 tmnxVdoMdaFccRetTotBwLmtCleared: VIDEO 1292
 tmnxVdoMdaFccRetTotBwLmtExceeded: VIDEO 1293
 tmnxVdoMdaFccRetTotSeLmtCleared: VIDEO 1293
 tmnxVdoMdaFccRetTotSeLmtExceeded: VIDEO 1294
 tmnxVdoMdaFccSesLimitCleared: VIDEO 1295
 tmnxVdoMdaFccSesLimitExceeded: VIDEO 1296
 tmnxVdoMdaRetBwLimitCleared: VIDEO 1296
 tmnxVdoMdaRetBwLimitExceeded: VIDEO 1297
 tmnxVdoMdaRetSesLimitCleared: VIDEO 1298
 tmnxVdoMdaRetSesLimitExceeded: VIDEO 1298
 tmnxVdoMdaSessionsLimitCleared: VIDEO 1299
 tmnxVdoMdaSessionsLimitExceeded: VIDEO 1300
 tmnxVdoMdaSGLimitCleared: VIDEO 1300

tmnxVdoMdaSGLimitExceeded: VIDEO 1301
 tmnxVdoVappFccBwLimitCleared: VIDEO 1301
 tmnxVdoVappFccBwLimitExceeded: VIDEO 1302
 tmnxVdoVappFccRetTotBwLmtCleared: VIDEO 1303
 tmnxVdoVappFccRetTotBwLmtExceeded: VIDEO 1304
 tmnxVdoVappFccRetTotSeLmtCleared: VIDEO 1304
 tmnxVdoVappFccRetTotSeLmtExceeded: VIDEO 1305
 tmnxVdoVappFccSesLimitCleared: VIDEO 1306
 tmnxVdoVappFccSesLimitExceeded: VIDEO 1306
 tmnxVdoVappRetBwLimitCleared: VIDEO 1307
 tmnxVdoVappRetBwLimitExceeded: VIDEO 1308
 tmnxVdoVappRetSesLimitCleared: VIDEO 1308
 tmnxVdoVappRetSesLimitExceeded: VIDEO 1309
 tmnxVdoVappSessionsLimitCleared: VIDEO 1310
 tmnxVdoVappSessionsLimitExceeded: VIDEO 1310
 tmnxVdoVappSGLimitCleared: VIDEO 1311
 tmnxVdoVappSGLimitExceeded: VIDEO 1312
 tmnxVrrpBecameBackup: VRRP 1313
 tmnxVrrpBfdIntfSessStateChgd: VRRP 1313
 tmnxVrrpIPListMismatch: VRRP 1314
 tmnxVrrpIPListMismatchClear: VRRP 1315
 tmnxVrrpMultipleOwners: VRRP 1315
 tmnxVrrpOperDownInvalidMac: VRRP 1316
 tmnxVrrpOperDownInvalidMacClear: VRRP 1317
 tmnxVRtrArpLmt: VRTR 1327
 tmnxVRtrArpThresholdExceeded: VRTR 1328
 tmnxVRtrBfdExtNoCpmNpResources: VRTR 1329
 tmnxVRtrBfdExtNoFreeTxIntrvlSlot: VRTR 1329
 tmnxVRtrBfdMaxSessionOnSlot: VRTR 1330
 tmnxVRtrBfdMultiHopFpMismatch: VRTR 1331
 tmnxVRtrBfdPortTypeNotSupported: VRTR 1332
 tmnxVRtrBfdSessExtDeleted: VRTR 1332
 tmnxVRtrBfdSessExtDown: VRTR 1333
 tmnxVRtrBfdSessExtProtChange: VRTR 1334
 tmnxVRtrBfdSessExtUp: VRTR 1334
 tmnxVRtrDHCP6AssignedIllegSubnet: DHCP 334
 tmnxVRtrDHCP6ClientMacUnresolved: DHCP 335
 tmnxVRtrDhcp6ClientStatusChanged: VRTR 1335
 tmnxVRtrDHCP6IllegalClientAddr: DHCP 335
 tmnxVRtrDHCP6LseStateOverride: DHCP 336
 tmnxVRtrDHCP6RelayLseStExceeded: DHCP 337
 tmnxVRtrDHCP6RelayReplyStripUni: DHCP 338
 tmnxVRtrDHCP6ServerLseStExceeded: DHCP 338
 tmnxVRtrDhcpClientStatusChanged: VRTR 1335
 tmnxVRtrDHCP6IfLseStatesExceeded: DHCP 339
 tmnxVRtrDHCP6SuspiciousPcktRcvd: DHCP 340
 tmnxVRtrDnsFault: VRTR 1336
 tmnxVRtrFibOccupancyThreshold: VRTR 1337
 tmnxVRtrFibVPNOccupancyThreshold: VRTR 1337
 tmnxVRtrGrExportLimitReached: VRTR 1338
 tmnxVRtrGrRoutesExpLimitDropped: VRTR 1339
 tmnxVRtrGrV6ExportLimitReached: VRTR 1339
 tmnxVRtrGrV6RoutesExpLimDropped: VRTR 1340
 tmnxVRtrHighRouteCleared: VRTR 1340
 tmnxVRtrHighRouteTCA: VRTR 1341
 tmnxVRtrIgnorePortState: VRTR 1342
 tmnxVRtrIfLdpSyncTimerStart: VRTR 1342
 tmnxVRtrIfLdpSyncTimerStop: VRTR 1343
 tmnxVRtrInetAddressAttachFailed: VRTR 1344
 tmnxVRtrIPv6HighRouteCleared: VRTR 1344
 tmnxVRtrIPv6HighRouteTCA: VRTR 1345
 tmnxVRtrIPv6MidRouteTCA: VRTR 1345
 tmnxVRtrIpv6NbrLmt: VRTR 1346
 tmnxVRtrIpv6NbrThresholdExceeded: VRTR 1347
 tmnxVRtrLeakExportLimitDropped: VRTR 1348
 tmnxVRtrLeakExportLimitReached: VRTR 1348
 tmnxVRtrMacAcctLimitCleared: VRTR 1349
 tmnxVRtrMacAcctLimitReached: VRTR 1349
 tmnxVRtrManagedRouteAddFailed: VRTR 1350
 tmnxVRtrMaxArpEntriesCleared: VRTR 1351
 tmnxVRtrMaxArpEntriesTCA: VRTR 1351
 tmnxVRtrMaxRoutes: VRTR 1352
 tmnxVRtrMcastMaxRoutesCleared: VRTR 1353
 tmnxVRtrMcastMaxRoutesTCA: VRTR 1353
 tmnxVRtrMcastMidRouteTCA: VRTR 1354
 tmnxVRtrMidRouteTCA: VRTR 1355
 tmnxVRtrNeDiscovered: VRTR 1355
 tmnxVRtrNeModified: VRTR 1356
 tmnxVRtrNeRemoved: VRTR 1357
 tmnxVRtrNgBfdNoCpmNpResources: VRTR 1358
 tmnxVRtrNgBfdSessDeleted: VRTR 1358
 tmnxVRtrNgBfdSessDown: VRTR 1359
 tmnxVRtrNgBfdSessProtChange: VRTR 1360
 tmnxVRtrNgBfdSessUp: VRTR 1360
 tmnxVRtrNHRvplsARPEXhaust: VRTR 1361
 tmnxVRtrNHRvplsARPHighUsage: VRTR 1362
 tmnxVRtrNHRvplsARPHighUsageClr: VRTR 1362
 tmnxVRtrPdnAddrMismatch: VRTR 1363
 tmnxVRtrPdnAddrMismatchCleared: VRTR 1364
 tmnxVRtrSingleSfmOverloadStateCh: VRTR 1365
 tmnxVRtrStaticRouteCPEStatus: VRTR 1365
 tmnxVRtrStaticRouteStatusChanged: VRTR 1366
 tmnxWlanGwBdCreated: WLAN_GW 1373
 tmnxWlanGwBdDeleted: WLAN_GW 1373
 tmnxWlanGwDsmGtpTunnelSetupFail: WLAN_GW 1374
 tmnxWlanGwGrpMemberUsageHigh: WLAN_GW 1375
 tmnxWlanGwGrpOperStateChanged: WLAN_GW 1375
 tmnxWlanGwGtpMessageDropped: WLAN_GW 1376
 tmnxWlanGwLomActive: WLAN_GW 1377
 tmnxWlanGwMgwConnected: WLAN_GW 1377
 tmnxWlanGwMgwRestarted: WLAN_GW 1378
 tmnxWlanGwMgwStateChanged: WLAN_GW 1379
 tmnxWlanGwNumMgwHi: WLAN_GW 1379
 tmnxWlanGwQosRadiusGtpMismatch: WLAN_GW 1380
 tmnxWlanGwResrcProblemCause: WLAN_GW 1381
 tmnxWlanGwResrcProblemDetected: WLAN_GW 1381
 tmnxWlanGwSubIfPmAddNewPIFailed: WLAN_GW 1382
 tmnxWlanGwSubIfPmCrIntObjFailed: WLAN_GW 1382
 tmnxWlanGwSubIfPmLsQryRtryFailed: WLAN_GW 1383
 tmnxWlanGwSubIfPmNewPIReqFailed: WLAN_GW 1384
 tmnxWlanGwSubIfPmPoolPartialUse: WLAN_GW 1384
 tmnxWlanGwSubIfPmPoolTimeout: WLAN_GW 1385
 tmnxWlanGwSubIfPmPoolUsageLow: WLAN_GW 1385
 tmnxWlanGwSubIfPmStartD6cFailed: WLAN_GW 1386

tmnxWlanGwSubIfRedActiveChanged: WLAN_GW 1387
 tmnxWlanGwTuQosProblem: WLAN_GW 1387
 tmnxWlanGwUeCreationFail: WLAN_GW 1388
 tmnxWlanGwUeReplacement: WLAN_GW 1389
 tmnxWlanNetworkConnected: PORT 863
 tmnxWlanNetworkDisconnected: PORT 864
 tmnxWppHostAuthenticationFailed: WPP 1390
 tmnxWppPGHostAuthFailed: WPP 1390
 tmnxWppPortalGroupStatChanged: WPP 1391
 tmnxWppPortalStatChanged: WPP 1392
 tmnxWppPortalUnreachable: WPP 1392
 topologyChangePipMajorState: STP 1063
 topologyChangePipState: STP 1063
 topologyChangeSapMajorState: STP 1064
 topologyChangeSapState: STP 1065
 topologyChangeVcpState: STP 1065
 tPortAccEgrQGrpHostMatchFailure: PORT 864
 tPortEgrVPortHostMatchFailure: PORT 865
 traceEvent: DEBUG 323
 trigPolicyPrevEval: ROUTE_POLICY 904
 tSecSgndSwUefiVarsUpdtReqd: SECURITY 1022
 tVrrpBecameBackup: VRRP 1317
 tVrrpPListMismatch: VRRP 1318
 tVrrpPListMismatchClear: VRRP 1319
 tVrrpMultipleOwners: VRRP 1319
 tVrrpOperDownInvalidMac: VRRP 1320
 tVrrpOperDownInvalidMacClear: VRRP 1321
 tVrrpPacketDiscarded: VRRP 1321
 tVrrpRouterAdvNotActivated: VRRP 1322
 tVrrpRouterAdvNotActivatedClear: VRRP 1323
 tVrrpTrapNewMaster: VRRP 1323
 vRtrIfDcpLocMonExcdAllDynAlloc: SECURITY 1029
 vRtrIfDcpLocMonExcdAllDynFreed: SECURITY 1030
 vRtrIfDcpLocMonExcdDynResource: SECURITY 1031
 vRtrIfDcpStaticConform: SECURITY 1032
 vRtrIfDcpStaticExcd: SECURITY 1032
 vRtrIfDcpStaticHoldDownEnd: SECURITY 1033
 vRtrIfDcpStaticHoldDownStart: SECURITY 1034
 vRtrIfDhcp6CISStateDnsChanged: VRTR 1368
 vRtrIfDhcpCIRtStatusChanged: VRTR 1368
 vRtrIfDhcpCISStateDnsChanged: VRTR 1369
 vRtrIfEthLoopbackStarted: VRTR 1370
 vRtrIfEthLoopbackStopped: VRTR 1370
 vrtrIfpTunnelOperStateChange: VRTR 1371
 vRtrIgmppGrpIfSapCModeRxQueryMism: IGMP 411
 vRtrIgmppGrpIfSapMaxGrpsLimExceed: IGMP 411
 vRtrIgmppGrpIfSapMaxGrpSrcLimExcd: IGMP 412
 vRtrIgmppGrpIfSapMaxSrcsLimExceed: IGMP 413
 vRtrIgmppGrpIfSapMcacPlyDropped: IGMP 414
 vRtrIgmppGrpIfSapRxQueryVerMism: IGMP 414
 vRtrIgmppHostCModeRxQueryMismatch: IGMP 415
 vRtrIgmppHostInstantiationFail: IGMP 416
 vRtrIgmppHostMaxGrpsLimitExceeded: IGMP 416
 vRtrIgmppHostMaxGrpSrcsLimitExcd: IGMP 417
 vRtrIgmppHostMaxSrcsLimitExceeded: IGMP 418
 vRtrIgmppHostMcacPlyDropped: IGMP 418
 vRtrIgmppHostQryIntervalConflict: IGMP 419
 vRtrIgmppHostRxQueryVerMismatch: IGMP 419
 vRtrIgmppIfCModeRxQueryMismatch: IGMP 420
 vRtrIgmppIfRxQueryVerMismatch: IGMP 421
 vRtrIgmppMaxGrpsLimitExceeded: IGMP 421
 vRtrIgmppMaxGrpSrcsLimitExceeded: IGMP 422
 vRtrIgmppMaxSrcsLimitExceeded: IGMP 423
 vRtrIgmppMcacPlyDropped: IGMP 423
 vRtrIgmppNotifyNumOfIPseclfHighWm: IGMP 424
 vRtrIgmppNotifyNumOfIPseclfLowWm: IGMP 425
 vRtrIgmppNotifyNumOfIPseclfMaxRch: IGMP 425
 vRtrIgmppSlaProfInstMcacPlyDrop: IGMP 426
 vRtrIisisSpbNbrMultAdjExists: ISIS 481
 vRtrIisisSpbNbrMultAdjExistsClear: ISIS 482
 vRtrLdpGroupIdMismatch: LDP 498
 vRtrLdpNgAddrFecCommMismatch: LDP 498
 vRtrLdpNgIfStateChange: LDP 499
 vRtrLdpNgInetIfStateChange: LDP 500
 vRtrLdpNgIpv4InstStateChange: LDP 500
 vRtrLdpNgIpv6InstStateChange: LDP 501
 vRtrLdpNgResourceExhaustion: LDP 502
 vRtrLdpNgSessionStateChange: LDP 503
 vRtrLdpNgSessMaxFecLimitReached: LDP 504
 vRtrLdpNgSessMaxFecThresChanged: LDP 505
 vRtrLdpNgTargPeerStateChange: LDP 506
 vRtrLdpStateChange: LDP 506
 vRtrMldGrpIfSapCModeRxQueryMism: MLD 642
 vRtrMldGrpIfSapMaxGrpsLimExceed: MLD 642
 vRtrMldGrpIfSapMaxGrpSrcLimExcd: MLD 643
 vRtrMldGrpIfSapMaxSrcsLimExceed: MLD 644
 vRtrMldGrpIfSapMcacPlyDropped: MLD 644
 vRtrMldGrpIfSapRxQueryVerMism: MLD 645

U

unacknowledgedTCN: STP 1066
 user_disconnect: SECURITY 1023

V

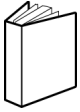
vcpActiveProtocolChange: STP 1067
 vrrpPacketDiscarded: VRRP 1324
 vrrpTrapAuthFailure: VRRP 1325
 vrrpTrapNewMaster: VRRP 1325
 vrrpTrapProtoError: VRRP 1326
 vRtrAutoCfgRaRtStatusChanged: VRTR 1367
 vRtrBgplInstanceError: VRTR 1367
 vRtrBierBfrldCollision: BIER 109
 vRtrBierMitMismatch: BIER 109
 vRtrBierSubDomainMismatch: BIER 110
 vRtrBierUnsupportedNhop: BIER 111
 vRtrIfDcpDynamicConform: SECURITY 1024
 vRtrIfDcpDynamicEnforceAlloc: SECURITY 1025
 vRtrIfDcpDynamicEnforceFreed: SECURITY 1025
 vRtrIfDcpDynamicExcd: SECURITY 1026
 vRtrIfDcpDynamicHoldDownEnd: SECURITY 1027
 vRtrIfDcpDynamicHoldDownStart: SECURITY 1028
 vRtrIfDcpLocMonExcd: SECURITY 1028

vRtrMldHostCModeRxQueryMismatch: MLD [646](#)
 vRtrMldHostInstantiationFail: MLD [647](#)
 vRtrMldHostMaxGrpsLimitExceeded: MLD [647](#)
 vRtrMldHostMaxGrpSrcsLimitExcd: MLD [648](#)
 vRtrMldHostMaxSrcsLimitExceeded: MLD [648](#)
 vRtrMldHostMcacPlcyDropped: MLD [649](#)
 vRtrMldHostQryIntervalConflict: MLD [650](#)
 vRtrMldHostRxQueryVerMismatch: MLD [650](#)
 vRtrMldIfCModeRxQueryMismatch: MLD [651](#)
 vRtrMldIfRxQueryVerMismatch: MLD [652](#)
 vRtrMldMaxGrpsLimitExceeded: MLD [652](#)
 vRtrMldMaxGrpSrcsLimitExceeded: MLD [653](#)
 vRtrMldMaxSrcsLimitExceeded: MLD [654](#)
 vRtrMldMcacPlcyDropped: MLD [654](#)
 vRtrMldSlaProfInstMcacPlcyDrop: MLD [655](#)
 vRtrMplsIfIPv6StateChange: MPLS [665](#)
 vRtrMplsIfStateChange: MPLS [665](#)
 vRtrMplsIPv6StateChange: MPLS [666](#)
 vRtrMplsLspActivePathChanged: MPLS [666](#)
 vRtrMplsLspDown: MPLS [667](#)
 vRtrMplsLspManualSwitchFailure: MPLS [668](#)
 vRtrMplsLspPathDown: MPLS [669](#)
 vRtrMplsLspPathLstFillReoptElig: MPLS [669](#)
 vRtrMplsLspPathManualDegStateChg: MPLS [670](#)
 vRtrMplsLspPathMbbStatusEvent: MPLS [670](#)
 vRtrMplsLspPathRerouted: MPLS [671](#)
 vRtrMplsLspPathResignaled: MPLS [672](#)
 vRtrMplsLspPathSoftPreempted: MPLS [672](#)
 vRtrMplsLspPathUp: MPLS [673](#)
 vRtrMplsLspResourceExhaustion: MPLS [673](#)
 vRtrMplsLspSwitchStbyFailure: MPLS [674](#)
 vRtrMplsLspUp: MPLS [675](#)
 vRtrMplsNodeInIgpOverload: MPLS [675](#)
 vRtrMplsNodeInIgpOverloadIpv6: MPLS [676](#)
 vRtrMplsP2mplInstanceDown: MPLS [677](#)
 vRtrMplsP2mplInstanceResignaled: MPLS [677](#)
 vRtrMplsP2mplInstanceUp: MPLS [678](#)
 vRtrMplsResignalTimerExpired: MPLS [679](#)
 vRtrMplsS2ISubLspDown: MPLS [679](#)
 vRtrMplsS2ISubLspPreempted: MPLS [680](#)
 vRtrMplsS2ISubLspRerouted: MPLS [680](#)
 vRtrMplsS2ISubLspResignaled: MPLS [681](#)
 vRtrMplsS2ISubLspUp: MPLS [682](#)
 vRtrMplsStateChange: MPLS [682](#)
 vRtrMplsTpLspActivePathChange: MPLS_TP [684](#)
 vRtrMplsTpLspActivePathUp: MPLS_TP [684](#)
 vRtrMplsTpLspPtTypeMismatchAlarm: MPLS_TP [685](#)
 vRtrMplsTpLspPtTypeMismatchClear: MPLS_TP [686](#)
 vRtrMplsTpLspRevertMismatchAlarm: MPLS_TP [686](#)
 vRtrMplsTpLspRevertMismatchClear: MPLS_TP [687](#)
 vRtrMplsXCBundleChange: MPLS [683](#)
 vRtrPimNgBierInbInvBfrId: PIM [788](#)
 vRtrPimNgBierInbInvSD: PIM [788](#)
 vRtrPimNgBSRStateChange: PIM [789](#)
 vRtrPimNgDataMtReused: PIM [790](#)
 vRtrPimNgGrpInSSMRange: PIM [790](#)
 vRtrPimNgHelloDropped: PIM [791](#)
 vRtrPimNgIfMaxNbrReached: PIM [791](#)
 vRtrPimNgIfNeighborLoss: PIM [792](#)
 vRtrPimNgIfNeighborUp: PIM [793](#)
 vRtrPimNgInstMaxNbrReached: PIM [793](#)
 vRtrPimNgInvalidIPmsiTunnel: PIM [794](#)
 vRtrPimNgInvalidJoinPrune: PIM [795](#)
 vRtrPimNgInvalidRegister: PIM [796](#)
 vRtrPimNgMaxGraftRetry: PIM [796](#)
 vRtrPimNgMaxGrpsLimitExceeded: PIM [797](#)
 vRtrPimNgMcacPlcyDropped: PIM [798](#)
 vRtrPimNgMDTLimitExceeded: PIM [798](#)
 vRtrPimNgReplicationLmtExceeded: PIM [799](#)
 vRtrPimNgSGLimitExceeded: PIM [799](#)
 vRtrPimNgUmhBMonFastFailPriToStb: PIM [800](#)
 vRtrPimNgUmhBMonFastFailStbToPri: PIM [801](#)
 vRtrRipAuthTypeFailure: RIP [891](#)
 vRtrRipAuthTypeMismatch: RIP [892](#)
 vRtrRipInstanceExpLmtReached: RIP [893](#)
 vRtrRipInstanceExpLmtWarning: RIP [893](#)
 vRtrRipInstanceRestarted: RIP [894](#)
 vRtrRipInstanceRtsExpLmtDropped: RIP [894](#)
 vRtrRipInstanceShuttingDown: RIP [895](#)
 vRtrRipPeerBfdDown: RIP [896](#)
 vRtrRsvplfNbrStateDown: RSVP [907](#)
 vRtrRsvplfNbrStateUp: RSVP [907](#)
 vRtrRsvplfStateChange: RSVP [908](#)
 vRtrRsvpPEFailOverPriToStdBy: RSVP [908](#)
 vRtrRsvpPEFailOverStdByToPri: RSVP [909](#)
 vRtrRsvpStateChange: RSVP [910](#)
 vRtrSpbEctFidCfgChg: ISIS [482](#)
 vRtrSrv6FunctionExhaustion: SRV6 [1046](#)
 vRtrSrv6LocatorResExhaustion: SRV6 [1046](#)
 vRtrSrv6SvcSidIndex: SRV6 [1047](#)
 vRtrTreeSidCdtPathActInsChanged: TREE_SID [1267](#)
 vRtrTreeSidCdtPathChanged: TREE_SID [1267](#)
 vRtrTreeSidFailOverPriToStdBy: TREE_SID [1268](#)
 vRtrTreeSidFailOverStdByToPri: TREE_SID [1269](#)
 vRtrTreeSidInSidRegFailure: TREE_SID [1269](#)
 vRtrTreeSidLabelRangeExhaustion: TREE_SID [1270](#)
 vRtrTreeSidLblRangeExhstCleared: TREE_SID [1271](#)
 vRtrTreeSidRepSegResExhaustion: TREE_SID [1271](#)
 vRtrTreeSidRepSegResExhstCleared: TREE_SID [1272](#)
 vRtrTreeSidTreeldAllocFailure: TREE_SID [1273](#)

W

warmStart: SNMP [1042](#)

Customer document and product support



Customer documentation

[Customer documentation welcome page](#)



Technical support

[Product support portal](#)



Documentation feedback

[Customer documentation feedback](#)