Nokia Service Router Linux

Release 24.3

Log Events Guide

3HE 20239 AAAA TQZZA
Edition: 01
March 2024

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

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.

Table of contents

1 About this guide

This document provides guidance for operators to interpret log events for the Nokia Service Router Linux (SR Linux). This document is intended for users who need to access and understand log events for SR Linux.

Note:
This manual covers the current release and may also contain some content that will be released in later maintenance loads. See the *SR Linux Release Notes* for information about features supported in each load.

Configuration and command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.

1.1 Precautionary and information messages

The following are information symbols used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.2 Conventions

Nokia SR Linux documentation uses the following command conventions.

- **Bold** indicates a command that the user must enter.
- Input and output examples are displayed in `Courier` text.
- An open right angle bracket indicates a progression of menu choices or simple command sequence (often selected from a user interface). Example: **start** > **connect to**
- A vertical bar (|) indicates a mutually exclusive argument.
- Square brackets ([ ]) indicate optional elements.

- Braces ({ }) indicate a required choice. When braces are contained within square brackets, they indicate a required choice within an optional element.
- *Italic* indicates a variable.

Generic IP addresses are used in examples. Replace these with the appropriate IP addresses used in the system.

2 Log events overview

This section provides general information about the log events described in this guide for the Nokia Service Router Linux (SR Linux).

For more information about logging, see the *SR Linux Configuration Basics Guide*.

2.1 Example log event

The following contains an example log event entry from this guide for the bgpNeighborBackwardTransition log event.

Table 1: bgpNeighborBackwardTransition properties

Property name	Value
Application name	bgp
Event name	bgpNeighborBackwardTransition
Default severity	warning
Message format string	In network-instance $network-instance$, the BGP session with $peer-address$ moved from higher state $last-state$ to lower state $session-state$ due to event $last-event$
Cause	No routes can be exchanged with this peer
Effect	N/A

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

Table 2: Log event entry field descriptions

Label	Description
Application name	Name of the application generating the log message
Event name	Name of the log event
Default severity	Severity level of the log event (see Table 3: Log event entry field descriptions for the severity level)
Message format string	Text description of the log event
Cause	Cause of the log event

Label	Description
Effect	Effect of the log event

2.2 Log event properties

Log events that are forwarded to a destination are formatted. All application-generated events have the following properties:

- time stamp in UTC or local time
- generating application
- router name identifying the VRF-ID that generated the event
- subject identifying the affected object
- short message describing the event

A log event with a memory, console, or file destination has the following format:

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

Format properties are described in Table 3: Log event entry field descriptions.

Table 3: Log event entry field descriptions

Label	Description
nnnn	Log event entry sequence number
YYYY/MM/DD	UTC or local date stamp for the log event entry: *YYYY* — Year *MM* — Month *DD* — Day
HH:MM:SS.SS	UTC time stamp for the event: *HH* — Hours (24-hour format) *MM* — Minutes *SS.SS* — Seconds.hundredths of a second
TZONE	Time zone (for example, UTC, EDT)
<severity>	Severity level of the log event: emerg — System is unusable alert — Action must be taken immediately crit — Critical conditions err — Error conditions

Label	Description
	warning — Warning conditions notice — Normal but significant condition info — Informational messages debug — Debug-level messages
<application>	Name of the application generating the log event message
<router>	Router name representing the VRF-ID that generated the log event
<subject>	Subject/affected object for the log event
<message>	Text description of the log event

3 What's new

Table 4: Event Changes

Event Name	Change
configUpdate	New
gnsiCredentialzRotateAccountCredentials	New
gnsiCredentialzRotateAccountCredentialsFinalized	New
gnsiCredentialzRotateAccountCredentialsInvalid	New
gnsiCredentialzRotateAccountCredentialsNotFinalized	New
gnsiCredentialzRotateHostParameters	New
gnsiCredentialzRotateHostParametersFinalized	New
gnsiCredentialzRotateHostParametersInvalid	New
gnsiCredentialzRotateHostParametersNotFinalized	New
grpcServerStart	New
grpcServerStop	New
subscriptionEnd	New
subscriptionRequestReceived	New
subscriptionStart	New
syncPTPParentChangeIP	New
unixSocketGrpcOperDown	New
unixSocketGrpcOperUp	New

4 aaa

4.1 serverDown

Table 5: serverDown properties

Property name	Value
Application name	aaa
Event name	serverDown
Default severity	error
Message format string	Server *server_address* in group *server_group* is down
Cause	The specified server is down, either via being unreachable, or a timeout.
Effect	The specified server can no longer be used for authentication, authorization, or accounting transactions.

4.2 serverGroupDown

Table 6: serverGroupDown properties

Property name	Value
Application name	aaa
Event name	serverGroupDown
Default severity	critical
Message format string	All servers in server group *server_group* are down
Cause	All servers within the specified server group are no longer available.
Effect	The specified server group can no longer be used for authentication, authorization, or accounting transactions.

4.3 serverRouteUnavailable

Table 7: serverRouteUnavailable properties

Property name	Value
Application name	aaa
Event name	serverRouteUnavailable
Default severity	error
Message format string	No route available to reach remote server *server_address* in server group *server_group* via network instance *network_instance*
Cause	No routes are available in the specified network instance to reach the remote server.
Effect	The specified server can no longer be used for authentication, authorization, or accounting transactions.

4.4 serverTimeout

Table 8: serverTimeout properties

Property name	Value
Application name	aaa
Event name	serverTimeout
Default severity	error
Message format string	Server *server_address* in group *server_group* has timed out
Cause	The connection between the AAA manager and the remote server has timed out. The server will be tried again in 30 seconds, or immediately if a valid response is received.
Effect	The specified server can no longer be used for authentication, authorization, or accounting transactions.

4.5 sessionClosed

Table 9: sessionClosed properties

Property name	Value
Application name	aaa
Event name	sessionClosed
Default severity	notice
Message format string	Closed session for user *user_name* from host *remote_host*
Cause	The specified user has closed a session on the system.
Effect	None.

4.6 sessionDisconnected

Table 10: sessionDisconnected properties

Property name	Value
Application name	aaa
Event name	sessionDisconnected
Default severity	notice
Message format string	Session for user *user_name* from remote host *remote_host* disconnected by administrative action
Cause	The specified user has been disconnected from the system by an administrators action.
Effect	The specified user is disconnected.

4.7 sessionOpened

Table 11: sessionOpened properties

Property name	Value
Application name	aaa
Event name	sessionOpened
Default severity	notice

Property name	Value
Message format string	Opened session for user *user_name* from host *remote_host*
Cause	The specified user has opened a session on the system.
Effect	None.

4.8 userAuthenticationFailed

Table 12: userAuthenticationFailed properties

Property name	Value
Application name	aaa
Event name	userAuthenticationFailed
Default severity	warning
Message format string	User *user_name* authentication failed from host *remote_host*
Cause	The specified user has failed authentication.
Effect	None.

4.9 userAuthenticationSucceeded

Table 13: userAuthenticationSucceeded properties

Property name	Value
Application name	aaa
Event name	userAuthenticationSucceeded
Default severity	notice
Message format string	User *user_name* successfully authenticated from host *remote_host*
Cause	The specified user has successfully authenticated.
Effect	None.

5 app

5.1 applicationFailed

Table 14: applicationFailed properties

Property name	Value
Application name	app
Event name	applicationFailed
Default severity	alert
Message format string	Application *application_name* has failed, *failure_count* of *failure_threshold* failures in the last *failure_window* seconds
Cause	The specified application has failed.
Effect	The specified application has failed, and all functionality it provides is inoperable. If this failure reaches the applications failure threshold then the applications failure action will be triggered, otherwise the application will be restarted.

5.2 applicationFailureActionTriggered

Table 15: applicationFailureActionTriggered properties

Property name	Value
Application name	app
Event name	applicationFailureActionTriggered
Default severity	alert
Message format string	Application *application_name* has failed *failure_threshold* times in the last *failure_window* seconds, triggering action *failure_action*
Cause	The specified application has failed enough times to trigger the applications failure action.
Effect	The applications failure action is triggered, as defined in the application-specific configuration.

5.3 applicationRestarted

Table 16: applicationRestarted properties

Property name	Value
Application name	app
Event name	applicationRestarted
Default severity	warning
Message format string	Restarted application *application_name*, restart type *restart_type*
Cause	Application manager has restarted the specified application.
Effect	The specified application has been restarted.

5.4 applicationStarted

Table 17: applicationStarted properties

Property name	Value
Application name	app
Event name	applicationStarted
Default severity	notice
Message format string	Successfully started application *application_name*
Cause	Application manager has started the specified application.
Effect	The specified application is started.

5.5 applicationStarting

Table 18: applicationStarting properties

Property name	Value
Application name	app
Event name	applicationStarting
Default severity	notice

Property name	**Value**
Message format string	Starting application *application_name*
Cause	Application manager is starting the specified application.
Effect	The specified application is starting.

6 acl

6.1 aclCpmIpv4MatchedPacket

Table 19: aclCpmIpv4MatchedPacket properties

Property name	Value
Application name	acl
Event name	aclCpmIpv4MatchedPacket
Default severity	notice
Message format string	An IPv4 packet, len *packet-length*, protocol *ip-protocol*, received by linecard *incoming-linecard* was *action* by entry *sequence-id* of the IPv4 cpm-filter. *source-ip*(*source-port*) -> *dest-ip*(*dest-port*)
Cause	This event is generated when an IPv4 packet matches an entry of the CPM IPv4 filter and that entry specifies a log action
Effect	None

6.2 aclCpmIpv6MatchedPacket

Table 20: aclCpmIpv6MatchedPacket properties

Property name	Value
Application name	acl
Event name	aclCpmIpv6MatchedPacket
Default severity	notice
Message format string	An IPv6 packet, len *packet-length*, protocol *last-next-header*, received by linecard *incoming-linecard* was *action* by entry *sequence-id* of the IPv6 cpm-filter. *source-ip*(*source-port*) -> *dest-ip*(*dest-port*)
Cause	This event is generated when an IPv6 packet matches an entry of the CPM IPv6 filter and that entry specifies a log action
Effect	None

6.3 aclInterfaceInputIpv4MatchedPacket

Table 21: aclInterfaceInputIpv4MatchedPacket properties

Property name	Value
Application name	acl
Event name	aclInterfaceInputIpv4MatchedPacket
Default severity	notice
Message format string	An IPv4 packet, len *packet-length*, protocol *ip-protocol*, received on *incoming-interface* was *action* by entry *sequence-id* of filter *filter-name*. *source-ip*(*source-port*) -> *dest-ip*(*dest-port*)
Cause	This event is generated when an IPv4 packet matches an entry of an IPv4 filter applied to ingress traffic on a subinterface and that entry specifies a log action
Effect	None

6.4 aclInterfaceInputIpv6MatchedPacket

Table 22: aclInterfaceInputIpv6MatchedPacket properties

Property name	Value
Application name	acl
Event name	aclInterfaceInputIpv6MatchedPacket
Default severity	notice
Message format string	An IPv6 packet, len *packet-length*, protocol *last-next-header*, received on *incoming-interface* was *action* by entry *sequence-id* of filter *filter-name*. *source-ip*(*source-port*) -> *dest-ip*(*dest-port*)
Cause	This event is generated when an IPv6 packet matches an entry of an IPv6 filter applied to ingress traffic on a subinterface and that entry specifies a log action
Effect	None

6.5 aclInterfaceOutputIpv4MatchedPacket

Table 23: aclInterfaceOutputIpv4MatchedPacket properties

Property name	**Value**
Application name	acl
Event name	aclInterfaceOutputIpv4MatchedPacket
Default severity	notice
Message format string	An IPv4 packet, len *packet-length*, protocol *ip-protocol*, intended for transmit on *outgoing-interface* was *action* by entry *sequence-id* of filter *filter-name*. *source-ip*(*source-port*) -> *dest-ip*(*dest-port*)
Cause	This event is generated when an IPv4 packet matches an entry of an IPv4 filter applied to egress traffic on a subinterface and that entry specifies a log action
Effect	None

6.6 aclInterfaceOutputIpv6MatchedPacket

Table 24: aclInterfaceOutputIpv6MatchedPacket properties

Property name	**Value**
Application name	acl
Event name	aclInterfaceOutputIpv6MatchedPacket
Default severity	notice
Message format string	An IPv6 packet, len *packet-length*, protocol *last-next-header*, intended for transmit on *outgoing-interface* was *action* by entry *sequence-id* of filter *filter-name*. *source-ip*(*source-port*) -> *dest-ip*(*dest-port*)
Cause	This event is generated when an IPv6 packet matches an entry of an IPv6 filter applied to egress traffic on a subinterface and that entry specifies a log action
Effect	None

6.7 aclTcamProgComplete

Table 25: aclTcamProgComplete properties

Property name	Value
Application name	acl
Event name	aclTcamProgComplete
Default severity	notice
Message format string	All TCAM banks on all linecards have been reprogrammed with the latest ACL configuration changes.
Cause	This event is generated when all TCAM banks on all linecards have been reprogrammed with the latest ACL configuration changes.
Effect	None

6.8 platformAclHighUtilization

Table 26: platformAclHighUtilization properties

Property name	Value
Application name	acl
Event name	platformAclHighUtilization
Default severity	warning
Message format string	The ACL resource called *resource-name* has reached *threshold*% or more utilization on linecard *linecard*, forwarding complex *forwarding-complex*. Only *free-entries* entries are remaining.
Cause	This event is generated when the utilization of an ACL resource has increased to a level that may warrant concern if futher resources are consumed
Effect	None

6.9 platformAclHighUtilizationLowered

Table 27: platformAclHighUtilizationLowered properties

Property name	Value
Application name	acl
Event name	platformAclHighUtilizationLowered
Default severity	notice
Message format string	The ACL resource called *resource-name* has decreased back to *threshold*% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*.
Cause	This event is generated when the utilization of an ACL resource has decreased to a level that may no longer warrant concern
Effect	None

6.10 platformTcamHighUtilization

Table 28: platformTcamHighUtilization properties

Property name	Value
Application name	acl
Event name	platformTcamHighUtilization
Default severity	warning
Message format string	The TCAM resource called *resource-name* has reached *threshold*% or more utilization on linecard *linecard*, forwarding complex *forwarding-complex*. Only *free-entries* entries are remaining.
Cause	This event is generated when the utilization of a TCAM resource has increased to a level that may warrant concern if futher resources are consumed
Effect	None

6.11 platformTcamHighUtilizationLowered

Table 29: platformTcamHighUtilizationLowered properties

Property name	Value
Application name	acl
Event name	platformTcamHighUtilizationLowered
Default severity	notice
Message format string	The TCAM resource called *resource-name* has decreased back to *threshold*% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*.
Cause	This event is generated when the utilization of a TCAM resource has decreased to a level that may no longer warrant concern
Effect	None

7 arpnd

7.1 ipArpEntryUpdated

Table 30: ipArpEntryUpdated properties

Property name	Value
Application name	arpnd
Event name	ipArpEntryUpdated
Default severity	informational
Message format string	The ARP entry for *ipv4-address* on *interface*.*subinterface-index* has been updated from mac *old-mac* type *old-type* to mac *new-mac* and type *new-type*.
Cause	This event is generated whenever an existing static or dynamic ARP entry for an IPv4 address is overwritten. This could be a triggered by a change of entry type (static vs dynamic) or a change of MAC address or a change of the subinterface binding.
Effect	None

7.2 ipSubinterfaceDuplicateIpv4Address

Table 31: ipSubinterfaceDuplicateIpv4Address properties

Property name	Value
Application name	arpnd
Event name	ipSubinterfaceDuplicateIpv4Address
Default severity	notice
Message format string	The IPv4 address *ipv4-address* assigned to *interface*.*subinterface-index* is being used by another host or router on the same subnet.
Cause	This event is generated when ARP detects that another system is using the same IPv4 address
Effect	Unreliable communications

7.3 ipSubinterfaceDuplicateIpv6Address

Table 32: ipSubinterfaceDuplicateIpv6Address properties

Property name	Value
Application name	arpnd
Event name	ipSubinterfaceDuplicateIpv6Address
Default severity	notice
Message format string	The IPv6 address *ipv6-address* assigned to *interface*.*subinterface-index* is being used by another host or router on the same subnet.
Cause	This event is generated when IPv6 DAD detects that another system is using the same IPv6 address
Effect	Unreliable communications

7.4 ipSubinterfaceDuplicateMacAddress

Table 33: ipSubinterfaceDuplicateMacAddress properties

Property name	Value
Application name	arpnd
Event name	ipSubinterfaceDuplicateMacAddress
Default severity	notice
Message format string	The MAC address *mac-address* used by *interface*.*subinterface-index* is being used by another host or router on the same subnet.
Cause	This event is generated when ARP or IPv6 Neighbor Discovery detects that another system is using the same MAC address
Effect	Unreliable communications

7.5 ipSubinterfaceInvalidArp

Table 34: ipSubinterfaceInvalidArp properties

Property name	Value
Application name	arpnd

Property name	Value
Event name	ipSubinterfaceInvalidArp
Default severity	notice
Message format string	An ARP request for *ipv4-address* was received on *interface*.*subinterface-index* and there is no matching IPv4 subnet.
Cause	This event is generated when ARP receives an ARP request for an invalid IPv4 address
Effect	None

7.6 ipSubinterfaceInvalidIpv6NeighborSolicitation

Table 35: ipSubinterfaceInvalidIpv6NeighborSolicitation properties

Property name	Value
Application name	arpnd
Event name	ipSubinterfaceInvalidIpv6NeighborSolicitation
Default severity	notice
Message format string	An IPv6 neighbor solicitation for *ipv6-address* was received on *interface*.*subinterface-index* and there is no matching IPv6 subnet.
Cause	This event is generated when IPv6 neighbor discovery receives a NS message for an invalid IPv6 address
Effect	None

7.7 ipv6NeighborEntryUpdated

Table 36: ipv6NeighborEntryUpdated properties

Property name	Value
Application name	arpnd
Event name	ipv6NeighborEntryUpdated
Default severity	informational
Message format string	The IPv6 neighbor discovery entry for *ipv6-address* on *interface*.*subinterface-index* has been updated from mac *old-mac* type *old-type* to mac *new-mac* and type *new-type*.

Property name	Value
Cause	This event is generated whenever an existing static or dynamic neighbor entry for an IPv6 address is overwritten. This could be a triggered by a change of entry type (static vs dynamic) or a change of MAC address or a change of the subinterface binding.
Effect	None

7.8 ipv6NeighborSubinterfaceLimit

Table 37: ipv6NeighborSubinterfaceLimit properties

Property name	Value
Application name	arpnd
Event name	ipv6NeighborSubinterfaceLimit
Default severity	warning
Message format string	The number of IPv6 neighbor discovery entries on *interface-dot-subindex* has reached the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of IPv6 neighbor entries in the subinterface is at the configured limit.
Effect	None

7.9 ipv6NeighborSubinterfaceLimitThreshold

Table 38: ipv6NeighborSubinterfaceLimitThreshold properties

Property name	Value
Application name	arpnd
Event name	ipv6NeighborSubinterfaceLimitThreshold
Default severity	warning
Message format string	The number of IPv6 neighbor discovery entries on *interface-dot-subindex* has reached *pct-threshold* percent of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of IPv6 neighbor entries in the subinterface is at the configured threshold warning limit.
Effect	None

8 bfd

8.1 bfdDownEvent

Table 39: bfdDownEvent properties

Property name	Value
Application name	bfd
Event name	bfdDownEvent
Default severity	warning
Message format string	BFD: Network-instance *network-instance* - Session from *local-address*:*local-discriminator* to *remote-address*:*remote-discriminator* has transitioned to the *down-state* state with local-diagnostic code: *local-diagnostic-str* (*local-diagnostic-code*) and remote-diagnostic code: *remote-diagnostic-str* (*remote-diagnostic-code*)
Cause	This notification is generated when a BFD session transitions to the Down or Admin Down state from an Up state.
Effect	The specified BFD session is now down. If the new state is Down, the session may be down due to a failure see the local or remote diagnostic code. If the new state is Admin-Down the session is down due to administrative reasons.

8.2 bfdMaxSessionActive

Table 40: bfdMaxSessionActive properties

Property name	Value
Application name	bfd
Event name	bfdMaxSessionActive
Default severity	warning
Message format string	BFD: Network-instance *network-instance* - Session from *local-address* to *remote-address* requested by *client-protocol* could not be created because the maximum number of BFD sessions *bfd-max-session* are active.

Property name	Value
Cause	This notification is generated when a BFD session cannot be created because the maximum number of BFD sessions are already active.
Effect	No more BFD sessions can be created until some existing sessions are removed.

8.3 bfdProtocolClientAdd

Table 41: bfdProtocolClientAdd properties

Property name	Value
Application name	bfd
Event name	bfdProtocolClientAdd
Default severity	notice
Message format string	BFD: Network-instance *network-instance* - The protocol *client-protocol* is now using BFD session from *local-address*:*local-discriminator* to *remote-address*: *remote-discriminator*
Cause	This notification is generated when a new protocol begins to use a BFD session to track liveliness.
Effect	The specified protocol will be notified by BFD if the associated sessions transitions from an Up to a Down state. It will be up to the receiving protocol to determine the course of action.

8.4 bfdProtocolClientRemove

Table 42: bfdProtocolClientRemove properties

Property name	Value
Application name	bfd
Event name	bfdProtocolClientRemove
Default severity	notice
Message format string	BFD: Network-instance *network-instance* - The protocol *client-protocol* using BFD session from *local-address*:*local-discriminator* to *remote-address*: *remote-discriminator* has been cleared

Property name	Value
Cause	This notification is generated when a protocol stops using a BFD session to track liveliness.
Effect	The specified protocol will no longer be notified by BFD if the associated sessions transitions from an Up to a Down state

8.5 bfdSessionDeleted

Table 43: bfdSessionDeleted properties

Property name	Value
Application name	bfd
Event name	bfdSessionDeleted
Default severity	notice
Message format string	BFD: Network-instance *network-instance* - Session from *local-address*:*local-discriminator* to *remote-address*:*remote-discriminator* has been deleted
Cause	This notification is generated when a BFD session has been removed from the configuration.
Effect	The BFD session has been removed.

8.6 bfdSessionUp

Table 44: bfdSessionUp properties

Property name	Value
Application name	bfd
Event name	bfdSessionUp
Default severity	notice
Message format string	BFD: Network-instance *network-instance* - Session from *local-address*:*local-discriminator* to *remote-address*:*remote-discriminator* is UP
Cause	This notification is generated when a BFD session transitions to the up state.
Effect	The BFD session is now operational.

8.7 bfdWarmrebootAdjustTimers

Table 45: bfdWarmrebootAdjustTimers properties

Property name	Value
Application name	bfd
Event name	bfdWarmrebootAdjustTimers
Default severity	notice
Message format string	BFD: Warm reboot adjustment of BFD timers initiated
Cause	This notification is generated when BFD is notified to adjust timers in preparation for warm reboot.
Effect	The timers on warm reboot capable BFD sessions are adjusted to keep the sessions UP during the warm reboot

8.8 bfdWarmrebootRestoreTimers

Table 46: bfdWarmrebootRestoreTimers properties

Property name	Value
Application name	bfd
Event name	bfdWarmrebootRestoreTimers
Default severity	notice
Message format string	BFD: Warm reboot restoration of BFD timers initiated
Cause	This notification is generated when BFD is notified to restore timers at completion of warm reboot.
Effect	The timers on warm reboot capable BFD sessions are restored to their configured values

8.9 microbfdDownEvent

Table 47: microbfdDownEvent properties

Property name	Value
Application name	bfd

Property name	Value
Event name	microbfdDownEvent
Default severity	warning
Message format string	BFD: LAG *lag-interface* member *member-interface* - Session from *local-address*:*local-discriminator* to *remote-address*:*remote-discriminator* has transitioned to the *down-state* state with local-diagnostic code: *local-diagnostic-str* (*local-diagnostic-code*) and remote-diagnostic code: *remote-diagnostic-str* (*remote-diagnostic-code*)
Cause	This notification is generated when a BFD session transitions to the Down or Admin Down state from an Up state.
Effect	The specified BFD session is now down. If the new state is Down, the session may be down due to a failure see the local or remote diagnostic code. If the new state is Admin-Down the session is down due to administrative reasons.

8.10 microbfdMaxSessionActive

Table 48: microbfdMaxSessionActive properties

Property name	Value
Application name	bfd
Event name	microbfdMaxSessionActive
Default severity	warning
Message format string	BFD: LAG *lag-interface* member *member-interface* - Session from *local-address* to *remote-address* could not be created because the maximum number of BFD sessions *bfd-max-session* are active.
Cause	This notification is generated when a BFD session cannot be created because the maximum number of BFD sessions are already active.
Effect	No more BFD sessions can be created until some existing sessions are removed.

8.11 microbfdSessionDeleted

Table 49: microbfdSessionDeleted properties

Property name	Value
Application name	bfd
Event name	microbfdSessionDeleted
Default severity	notice
Message format string	BFD: LAG *lag-interface* member *member-interface* - Session from *local-address*:*local-discriminator* to *remote-address*:*remote-discriminator* has been deleted
Cause	This notification is generated when a BFD session has been removed from the configuration.
Effect	The BFD session has been removed.

8.12 microbfdSessionUp

Table 50: microbfdSessionUp properties

Property name	Value
Application name	bfd
Event name	microbfdSessionUp
Default severity	notice
Message format string	BFD: LAG *lag-interface* member *member-interface* - Session from *local-address*:*local-discriminator* to *remote-address*:*remote-discriminator* is UP
Cause	This notification is generated when a BFD session transitions to the up state.
Effect	The BFD session is now operational.

8.13 sbfdechoDownEvent

Table 51: sbfdechoDownEvent properties

Property name	Value
Application name	bfd
Event name	sbfdechoDownEvent
Default severity	warning
Message format string	BFD: BFD: SR Policy Id *policy-id* Policy Name *policy-name* User Type *user-type* Endpoint *endpoint* Network-instance *network-instance* - SBFD Echo Session discriminator *local-discriminator* has transitioned to the *down-state* state with local-diagnostic code: *local-diagnostic-str* (*local-diagnostic-code*)
Cause	This notification is generated when a BFD session transitions to the Down or Admin Down state from an Up state.
Effect	The specified BFD session is now down. If the new state is Down, the session may be down due to a failure see the local or remote diagnostic code. If the new state is Admin-Down the session is down due to administrative reasons.

8.14 sbfdechoMaxSessionActive

Table 52: sbfdechoMaxSessionActive properties

Property name	Value
Application name	bfd
Event name	sbfdechoMaxSessionActive
Default severity	warning
Message format string	BFD: SR Policy Id *policy-id* Policy Name *policy-name* User Type *user-type* Endpoint *endpoint* Network-instance *network-instance* - SBFD Echo Session requested by *client-protocol* could not be created because the maximum number of BFD sessions *bfd-max-session* are active.
Cause	This notification is generated when a BFD session cannot be created because the maximum number of BFD sessions are already active.
Effect	No more BFD sessions can be created until some existing sessions are removed.

8.15 sbfdechoSessionDeleted

Table 53: sbfdechoSessionDeleted properties

Property name	Value
Application name	bfd
Event name	sbfdechoSessionDeleted
Default severity	notice
Message format string	BFD: SR Policy Id *policy-id* Policy Name *policy-name* User Type *user-type* Endpoint *endpoint* Network-instance *network-instance* - SBFD Echo Session discriminator *local-discriminator* has been deleted
Cause	This notification is generated when a BFD session has been removed from the configuration.
Effect	The BFD session has been removed.

8.16 sbfdechoSessionUp

Table 54: sbfdechoSessionUp properties

Property name	Value
Application name	bfd
Event name	sbfdechoSessionUp
Default severity	notice
Message format string	BFD: SR Policy Id *policy-id* Policy Name *policy-name* User Type *user-type* Endpoint *endpoint* Network-instance *network-instance* - SBFD Echo Session discriminator *local-discriminator* is UP
Cause	This notification is generated when a BFD session transitions to the up state.
Effect	The BFD session is now operational.

9 bgp

9.1 bgpIncomingDynamicPeerLimitReached

Table 55: bgpIncomingDynamicPeerLimitReached properties

Property name	Value
Application name	bgp
Event name	bgpIncomingDynamicPeerLimitReached
Default severity	notice
Message format string	In network-instance *network-instance*, an incoming BGP connection from *peer-address* was rejected because the limit for the maximum number of incoming dynamic peers, *max-sessions*, has been reached.
Cause	The configured limit on the number of incoming sessions associated with dynamic peers has been reached.
Effect	The incoming connection attempt is rejected.

9.2 bgpIncomingInterfaceDynamicPeerLimitReached

Table 56: bgpIncomingInterfaceDynamicPeerLimitReached properties

Property name	Value
Application name	bgp
Event name	bgpIncomingInterfaceDynamicPeerLimitReached
Default severity	notice
Message format string	In network-instance *network-instance*, an incoming BGP connection from *peer-address* was rejected because the limit for the maximum number of incoming interface dynamic peers, *max-sessions*, has been reached for the interface *interface*.
Cause	This event is generated when the dynamic session limit for this interface is reached.
Effect	The incoming connection attempt is rejected.

9.3 bgpInstanceConvergenceStateTransition

Table 57: bgpInstanceConvergenceStateTransition properties

Property name	Value
Application name	bgp
Event name	bgpInstanceConvergenceStateTransition
Default severity	notice
Message format string	In network-instance *network-instance*, the BGP convergence state for the *address-family* address family transitioned from the *previous-state* state to the *new-state* state
Cause	This event is generated when the BGP convergence process is being tracked and a state transition occurs
Effect	Dependent on the new state

9.4 bgpLowMemory

Table 58: bgpLowMemory properties

Property name	Value
Application name	bgp
Event name	bgpLowMemory
Default severity	critical
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* was terminated immediately because BGP has out of memory.
Cause	BGP has run out of memory and this peer has been shutdown to reclaim some memory.
Effect	No routes can be exchanged with this peer.

9.5 bgpNeighborBackwardTransition

Table 59: bgpNeighborBackwardTransition properties

Property name	Value
Application name	bgp
Event name	bgpNeighborBackwardTransition
Default severity	warning
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* moved from higher state *last-state* to lower state *session-state* due to event *last-event*
Cause	This event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.
Effect	No routes can be exchanged with this peer.

9.6 bgpNeighborClosedTCPConn

Table 60: bgpNeighborClosedTCPConn properties

Property name	Value
Application name	bgp
Event name	bgpNeighborClosedTCPConn
Default severity	warning
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* was closed because the neighbor closed the TCP connection.
Cause	The router received a TCP FIN message from its peer.
Effect	No routes can be exchanged with this peer.

9.7 bgpNeighborEstablished

Table 61: bgpNeighborEstablished properties

Property name	Value
Application name	bgp
Event name	bgpNeighborEstablished

Property name	Value
Default severity	notice
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* moved into the ESTABLISHED state
Cause	The BGP session entered the ESTABLISHED state.
Effect	Routes of negotiated address families can now be exchanged with this peer.

9.8 bgpNeighborGRHelpingStarted

Table 62: bgpNeighborGRHelpingStarted properties

Property name	Value
Application name	bgp
Event name	bgpNeighborGRHelpingStarted
Default severity	notice
Message format string	In network-instance *network-instance*, the router has started providing GR helper service to the neighbor *peer-address*
Cause	GR helper is activated
Effect	Routes previously received from the peer, prior to its restart, are retained as stale until the stale-routes-time expires.

9.9 bgpNeighborGRHelpingStopped

Table 63: bgpNeighborGRHelpingStopped properties

Property name	Value
Application name	bgp
Event name	bgpNeighborGRHelpingStopped
Default severity	notice
Message format string	In network-instance *network-instance*, the router has stopped providing GR helper service to the neighbor *peer-address*
Cause	GR helper is deactivated

Property name	Value
Effect	Any remaining stale routes are immediately removed.

9.10 bgpNeighborHoldTimeExpired

Table 64: bgpNeighborHoldTimeExpired properties

Property name	Value
Application name	bgp
Event name	bgpNeighborHoldTimeExpired
Default severity	warning
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* was terminated because a KEEPALIVE message was not received before the holdtime limit of *negotiated-hold-time* was reached.
Cause	BGP did not receive a KEEPALIVE message from the peer before the negotiated holdtime expired.
Effect	No routes can be exchanged with this peer.

9.11 bgpNeighborInvalidLocalIP

Table 65: bgpNeighborInvalidLocalIP properties

Property name	Value
Application name	bgp
Event name	bgpNeighborInvalidLocalIP
Default severity	warning
Message format string	In network-instance *network-instance*, an incoming BGP connection from *peer-address* was rejected because the destination IP address does not match the allowed local-address, *local-address*.
Cause	BGP configuration does not allow an incoming BGP connection to this IP address.
Effect	No routes can be exchanged with this peer.

9.12 bgpNeighborNoOpenReceived

Table 66: bgpNeighborNoOpenReceived properties

Property name	Value
Application name	bgp
Event name	bgpNeighborNoOpenReceived
Default severity	warning
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* was terminated because an OPEN message was not received before the configured holdtime limit was reached.
Cause	BGP did not receive an OPEN message from the peer before the configured holdtime expired.
Effect	No routes can be exchanged with this peer.

9.13 bgpNeighborPrefixLimitReached

Table 67: bgpNeighborPrefixLimitReached properties

Property name	Value
Application name	bgp
Event name	bgpNeighborPrefixLimitReached
Default severity	notice
Message format string	In network-instance *network-instance*, the number of *family* routes received from the neighbor *peer-address* has exceeded the configured limit.
Cause	The number of received routes from the peer has exceeded the configured limit for the associated address family.
Effect	No effect. Routes above the limit are still received and processed.

9.14 bgpNeighborPrefixLimitThresholdReached

Table 68: bgpNeighborPrefixLimitThresholdReached properties

Property name	Value
Application name	bgp
Event name	bgpNeighborPrefixLimitThresholdReached
Default severity	notice
Message format string	In network-instance *network-instance*, the number of *family* routes received from the neighbor *peer-address* has exceeded the configured threshold, which is *warning-threshold-pct*% of the limit.
Cause	The number of received routes from the peer has exceeded the configured threshold for the associated address family.
Effect	No effect. Routes above the threshold are still received and processed.

9.15 bgpNeighborUnknownRemoteIP

Table 69: bgpNeighborUnknownRemoteIP properties

Property name	Value
Application name	bgp
Event name	bgpNeighborUnknownRemoteIP
Default severity	warning
Message format string	In network-instance *network-instance*, an incoming BGP connection from *peer-address* was rejected because the source IP address does not match the address of any configured neighbor or any dynamic-neighbor block.
Cause	BGP configuration does not allow an incoming BGP connection from this IP address.
Effect	No routes can be exchanged with this peer.

9.16 bgpNLRIInvalid

Table 70: bgpNLRIInvalid properties

Property name	Value
Application name	bgp
Event name	bgpNLRIInvalid
Default severity	warning
Message format string	In network-instance *network-instance*, a route for NLRI *nlri* was received from neighbor *peer-address* and it was ignored because it is considered an invalid NLRI.
Cause	The router received an UPDATE with an invalid NLRI
Effect	The route associated with the NLRI is not added or removed from the BGP RIB.

9.17 bgpNotificationReceivedFromNeighbor

Table 71: bgpNotificationReceivedFromNeighbor properties

Property name	Value
Application name	bgp
Event name	bgpNotificationReceivedFromNeighbor
Default severity	warning
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* was closed because the neighbor sent a NOTIFICATION with code *last-notification-error-code* and subcode *last-notification-error-subcode*
Cause	The router received a NOTIFICATION message from its peer.
Effect	No routes can be exchanged with this peer.

9.18 bgpNotificationSentToNeighbor

Table 72: bgpNotificationSentToNeighbor properties

Property name	Value
Application name	bgp
Event name	bgpNotificationSentToNeighbor
Default severity	warning
Message format string	In network-instance *network-instance*, the BGP session with *peer-address* was closed because the router sent this neighbor a NOTIFICATION with code *last-notification-error-code* and subcode *last-notification-error-subcode*
Cause	The router sent a NOTIFICATION message to its peer.
Effect	No routes can be exchanged with this peer.

9.19 bgpOutgoingDynamicPeerLimitReached

Table 73: bgpOutgoingDynamicPeerLimitReached properties

Property name	Value
Application name	bgp
Event name	bgpOutgoingDynamicPeerLimitReached
Default severity	notice
Message format string	In network-instance *network-instance*, no session was initiated towards the LLDP-discovered address *peer-address* because the limit for the maximum number of outgoing dynamic peers, *max-sessions*, has been reached.
Cause	The configured limit on the number of outgoing sessions associated with dynamic peers has been reached.
Effect	No connection attempt is made by the router.

9.20 bgpPathAttributeDiscarded

Table 74: bgpPathAttributeDiscarded properties

Property name	Value
Application name	bgp
Event name	bgpPathAttributeDiscarded
Default severity	warning
Message format string	In network-instance *network-instance*, a path attribute of type *attribute-type* and length *attribute-length* was discarded in a route received from the neighbor *peer-address*.
Cause	The path attribute was malformed and the attribute-discard approach is used for this type of attribute.
Effect	The intended meaning of that path attribute is not applied but the UPDATE message is still processed for new reachabiity information.

9.21 bgpPathAttributeMalformed

Table 75: bgpPathAttributeMalformed properties

Property name	Value
Application name	bgp
Event name	bgpPathAttributeMalformed
Default severity	warning
Message format string	In network-instance *network-instance*, a path attribute of type *attribute-type* and length *attribute-length* that was received in a route from the neighbor *peer-address* was considered malformed.
Cause	The router considers a path attribute to be malformed, for example not the expected length. The UPDATE message can still be parsed though.
Effect	Dependent on the type of the malformed path attribute. Either the malformed attribute is discarded or else the entire UPDATE message is considered to have unreachable NLRI.

9.22 bgpRouteWithdrawnDueToError

Table 76: bgpRouteWithdrawnDueToError properties

Property name	Value
Application name	bgp
Event name	bgpRouteWithdrawnDueToError
Default severity	warning
Message format string	In network-instance *network-instance*, a route for NLRI *nlri* was received from neighbor *peer-address* and it was considered withdrawn because of a recoverable error in the UPDATE message.
Cause	The router received a malformed UPDATE and the malformed path attribute(s) require as a treat-as-withdraw error handling behavior for the included set of routes.
Effect	There is no reachability for the NLRI in the malformed UPDATE message.

9.23 bgpUpdateInvalid

Table 77: bgpUpdateInvalid properties

Property name	Value
Application name	bgp
Event name	bgpUpdateInvalid
Default severity	warning
Message format string	In network-instance *network-instance*, an UPDATE message received from neighbor *peer-address* was considered invalid and caused the connection to be closed because the NLRI could not be parsed correctly.
Cause	The router received a malformed UPDATE which made it is impossible to identify all of the NLRI correctly.
Effect	The session is shutdown.

10 bridgetable

10.1 evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitHighUtilization

Table 78: evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitHighUtilization
Default severity	warning
Message format string	The number of Evpn-Mpls Multicast Destinations in the bridge table for bgp-instance *bgp-instance* on network-instance *network-instance* has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Evpn-Mpls Multicast Destinations in the bgp-instance reaches the warning threshold percentage of the allowed limit.
Effect	None

10.2 evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitHighUtilizationLow

Table 79: evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of Evpn-Mpls Multicast Destinations in the bridge table for bgp-instance *bgp-instance* on network-instance *network-instance* is now below a *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Evpn-Mpls Multicast Destinations in the bgp-instance is 5% below the warning threshold

Property name	Value
	percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.3 evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitLowered

Table 80: evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitLowered properties

Property name	Value
Application name	bridgetable
Event name	evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitLowered
Default severity	notice
Message format string	The number of Evpn-Mpls Multicast Destinations in the bridge table for bgp-instance *bgp-instance* on network-instance *network-instance* is now below the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Evpn-Mpls Multicast Destinations in a bgp-instance goes below the allowed limit, after being above the allowed limit
Effect	New Evpn-Mpls Multicast Destinations can be added to the multicast list of the network-instance.

10.4 evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitReached

Table 81: evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitReached properties

Property name	Value
Application name	bridgetable
Event name	evpnMplsBgpInstanceBridgeTableMulticastDestinationsLimitReached
Default severity	warning
Message format string	The number of Evpn-Mpls Multicast Destinations in the bridge table for bgp-instance *bgp-instance* on network-instance *network-instance* is at the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Evpn-Mpls Multicast Destinations in a bgp-instance is at the allowed limit.

Property name	Value
Effect	New Evpn-Mpls Multicast Destinations cannot be added to the multicast list of the network-instance.

10.5 l2SubinterfaceBridgeTableDuplicateMacAddressDeleted

Table 82: l2SubinterfaceBridgeTableDuplicateMacAddressDeleted properties

Property name	Value
Application name	bridgetable
Event name	l2SubinterfaceBridgeTableDuplicateMacAddressDeleted
Default severity	notice
Message format string	A duplicate MAC address *mac-address* detected on sub-interface *interface*.*subinterface-index* is now deleted.
Cause	This event is generated when a duplicate MAC address is deleted.
Effect	The duplicate mac-address is now deleted.

10.6 l2SubinterfaceBridgeTableDuplicateMacAddressDetected

Table 83: l2SubinterfaceBridgeTableDuplicateMacAddressDetected properties

Property name	Value
Application name	bridgetable
Event name	l2SubinterfaceBridgeTableDuplicateMacAddressDetected
Default severity	notice
Message format string	A duplicate MAC address *mac-address* was detected on sub-interface *interface*.*subinterface-index*.
Cause	This event is generated when a duplicate MAC address is detected, qualified by the bridge-table mac-duplication configuration under the network-instance and the sub-interfaces configured under the network-instance.
Effect	depending on the mac-duplication configuration, traffic destined to the duplicate mac-address maybe blackholed or not reprogrammed against any other sub-interface on the network-instance

10.7 l2SubinterfaceBridgeTableMacLimitHighUtilization

Table 84: l2SubinterfaceBridgeTableMacLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	l2SubinterfaceBridgeTableMacLimitHighUtilization
Default severity	warning
Message format string	The number of MAC addresses in the bridge table for sub-interface *interface*.*subinterface-index* has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table for a sub-interface reaches the configured warning threshold percentage of the allowed limit.
Effect	None

10.8 l2SubinterfaceBridgeTableMacLimitHighUtilizationLowered

Table 85: l2SubinterfaceBridgeTableMacLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	l2SubinterfaceBridgeTableMacLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of MAC addresses in the bridge table for sub-interface *interface*.*subinterface-index* is below *pct-threshold*% (minus 5%) of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table for a sub-interface is below 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.9 l2SubinterfaceBridgeTableMacLimitLowered

Table 86: l2SubinterfaceBridgeTableMacLimitLowered properties

Property name	Value
Application name	bridgetable
Event name	l2SubinterfaceBridgeTableMacLimitLowered
Default severity	notice
Message format string	The number of MAC addresses in the bridge table for the sub-interface *interface*.*subinterface-index* is below the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table for a sub-interface is below the allowed limit, after being above the allowed limit
Effect	new mac-addresses for the sub-interface can now be added to the bridge table.

10.10 l2SubinterfaceBridgeTableMacLimitReached

Table 87: l2SubinterfaceBridgeTableMacLimitReached properties

Property name	Value
Application name	bridgetable
Event name	l2SubinterfaceBridgeTableMacLimitReached
Default severity	warning
Message format string	The number of MAC addresses in the bridge table for the sub-interface *interface*.*subinterface-index* has reached the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table for the sub-interface is at the allowed limit.
Effect	new mac-addresses for the sub-interface cannot be added in the bridge table.

10.11 networkInstanceBridgeTableDuplicateMacAddressDeleted

Table 88: networkInstanceBridgeTableDuplicateMacAddressDeleted properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableDuplicateMacAddressDeleted
Default severity	notice
Message format string	A duplicate MAC address *mac-address* detected on *network-instance* is now deleted.
Cause	This event is generated when a duplicate MAC address is deleted.
Effect	The duplicate mac-address is now deleted.

10.12 networkInstanceBridgeTableDuplicateMacAddressDetected

Table 89: networkInstanceBridgeTableDuplicateMacAddressDetected properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableDuplicateMacAddressDetected
Default severity	notice
Message format string	A duplicate MAC address *mac-address* was detected on *network-instance*.
Cause	This event is generated when a duplicate MAC address is detected, qualified by the bridge-table mac-duplication configuration under the network-instance and the sub-interfaces configured under the network-instance.
Effect	depending on the mac-duplication configuration, traffic destined to the duplicate mac-address maybe blackholed or not reprogrammed against any other sub-interface on the network-instance

10.13 networkInstanceBridgeTableMacLimitHighUtilization

Table 90: networkInstanceBridgeTableMacLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableMacLimitHighUtilization
Default severity	warning
Message format string	The number of MAC addresses in the bridge table of network-instance *network-instance* has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of a network-instance reaches the configured warning threshold percentage of the allowed limit.
Effect	None

10.14 networkInstanceBridgeTableMacLimitHighUtilizationLowered

Table 91: networkInstanceBridgeTableMacLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableMacLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of MAC addresses in the bridge table of network-instance *network-instance* is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of the network-instance is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.15 networkInstanceBridgeTableMacLimitLowered

Table 92: networkInstanceBridgeTableMacLimitLowered properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableMacLimitLowered
Default severity	notice
Message format string	The number of MAC addresses in the bridge table of network-instance *network-instance* is now below the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of a network-instance goes below the allowed limit, after being above the allowed limit
Effect	new mac-addresses can now be added to the bridge table.

10.16 networkInstanceBridgeTableMacLimitReached

Table 93: networkInstanceBridgeTableMacLimitReached properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableMacLimitReached
Default severity	warning
Message format string	The number of MAC addresses in the bridge table of network-instance *network-instance* is at the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of a network-instance is at the allowed limit.
Effect	new mac-addresses cannot be added in the bridge table.

10.17 networkInstanceBridgeTableProxyArpLimitHighUtilization

Table 94: networkInstanceBridgeTableProxyArpLimitHighUtilization properties

Property name	Value
Application name	bridgetable

Property name	Value
Event name	networkInstanceBridgeTableProxyArpLimitHighUtilization
Default severity	warning
Message format string	The number of proxy ARP entries in the bridge table of network-instance *network-instance* has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ARP entries in the bridge table of a network-instance reaches the warning threshold percentage of the allowed limit.
Effect	None

10.18 networkInstanceBridgeTableProxyArpLimitHighUtilizationLowered

Table 95: networkInstanceBridgeTableProxyArpLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyArpLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of proxy ARP entries in the bridge table of network-instance *network-instance* is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ARP entriesin the bridge table of the network-instance is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.19 networkInstanceBridgeTableProxyArpNdDuplicateIpAddressDeleted

Table 96: networkInstanceBridgeTableProxyArpNdDuplicateIpAddressDeleted properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyArpNdDuplicateIpAddressDeleted

Property name	Value
Default severity	notice
Message format string	A duplicate proxy IP *ip-address* detected on *network-instance* is now deleted.
Cause	This event is generated when a duplicate proxy IP is deleted.
Effect	The duplicate proxy IP is now deleted.

10.20 networkInstanceBridgeTableProxyArpNdDuplicateIpAddressDetected

Table 97: networkInstanceBridgeTableProxyArpNdDuplicateIpAddressDetected properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyArpNdDuplicateIpAddressDetected
Default severity	notice
Message format string	A duplicate link-layer-address *new-mac-address* was detected for proxy IP *ip-address* link-layer-address *old-mac-address* on *network-instance*.
Cause	This event is generated when when duplicate detection criteria is met when a new link-layer-address overwrites the existing link-layer-address for the proxy IP on the network-instance.
Effect	A traffic disruption may occur if both systems are active

10.21 networkInstanceBridgeTableProxyNdLimitHighUtilization

Table 98: networkInstanceBridgeTableProxyNdLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyNdLimitHighUtilization
Default severity	warning
Message format string	The number of proxy ND entries in the bridge table of network-instance *network-instance* has reached *pct-threshold*% of the allowed limit of *maximum-entries*.

Property name	Value
Cause	This event is generated when the number of proxy ND entries in the bridge table of a network-instance reaches the warning threshold percentage of the allowed limit.
Effect	None

10.22 networkInstanceBridgeTableProxyNdLimitHighUtilizationLowered

Table 99: networkInstanceBridgeTableProxyNdLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyNdLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of proxy ND entries in the bridge table of network-instance *network-instance* is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ND entriesin the bridge table of the network-instance is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.23 systemBridgeTableMacLimitHighUtilization

Table 100: systemBridgeTableMacLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableMacLimitHighUtilization
Default severity	warning
Message format string	The number of MAC addresses in the bridge table of the system has reached *pct-threshold*% of the allowed limit of *maximum-entries*.

Property name	Value
Cause	This event is generated when the number of MAC addresses in the bridge table of the system reaches the configured warning threshold percentage of the allowed limit.
Effect	None

10.24 systemBridgeTableMacLimitHighUtilizationLowered

Table 101: systemBridgeTableMacLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableMacLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of MAC addresses in the bridge table of the system is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of the system is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.25 systemBridgeTableMacLimitLowered

Table 102: systemBridgeTableMacLimitLowered properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableMacLimitLowered
Default severity	notice
Message format string	The number of MAC addresses in the bridge table of the system is now below the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of the system goes below the allowed limit, after being above the allowed limit

Property name	Value
Effect	new mac-addresses can now be added to the bridge table.

10.26 systemBridgeTableMacLimitReached

Table 103: systemBridgeTableMacLimitReached properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableMacLimitReached
Default severity	warning
Message format string	The number of MAC addresses in the bridge table of the system is at the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of MAC addresses in the bridge table of the system is at the allowed limit.
Effect	new mac-addresses cannot be added in any bridge table in the system.

10.27 systemBridgeTableProxyArpLimitHighUtilization

Table 104: systemBridgeTableProxyArpLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableProxyArpLimitHighUtilization
Default severity	warning
Message format string	The number of proxy ARP entries in the bridge table of the system has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ARP entries in the bridge table the system reaches the warning threshold percentage of the allowed limit.
Effect	None

10.28 systemBridgeTableProxyArpLimitHighUtilizationLowered

Table 105: systemBridgeTableProxyArpLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableProxyArpLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of proxy ARP entries in the bridge table of the system is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ARP entriesin the bridge table of the system is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.29 systemBridgeTableProxyNdLimitHighUtilization

Table 106: systemBridgeTableProxyNdLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableProxyNdLimitHighUtilization
Default severity	warning
Message format string	The number of proxy ND entries in the bridge table of the system has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ND entries in the bridge table the system reaches the warning threshold percentage of the allowed limit.
Effect	None

10.30 systemBridgeTableProxyNdLimitHighUtilizationLowered

Table 107: systemBridgeTableProxyNdLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableProxyNdLimitHighUtilizationLowered
Default severity	notice
Message format string	The number of proxy ND entries in the bridge table of the system is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of proxy ND entries in the bridge table of the system is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.31 systemMulticastIdLimitHighUtilization

Table 108: systemMulticastIdLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	systemMulticastIdLimitHighUtilization
Default severity	warning
Message format string	The multicast id usage of the system has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the multicast id usage of the system reaches the configured warning threshold percentage of the allowed limit.
Effect	None

10.32 systemMulticastIdLimitHighUtilizationLowered

Table 109: systemMulticastIdLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	systemMulticastIdLimitHighUtilizationLowered
Default severity	notice
Message format string	The multicast id usage of the system is now at *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the multicast id usage of the system is at 5% minus the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.33 vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilization

Table 110: vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilization
Default severity	warning
Message format string	The number of Vxlan Multicast Destinations in the bridge table for the vxlan-interface *tunnel-interface*.*vxlan-interface* has reached *pct-threshold*% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Vxlan Multicast Destinations in the vxlan-interface reaches the warning threshold percentage of the allowed limit.
Effect	None

10.34 vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilizationLowered

Table 111: vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilizationLowered properties

Property name	Value
Application name	bridgetable
Event name	vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilization Lowered
Default severity	notice
Message format string	The number of Vxlan Multicast Destinations in the bridge table for the vxlan-interface *tunnel-interface*.*vxlan-interface* is now below a *pct-threshold*% minus 5% of the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Vxlan Multicast Destinations in the vxlan-interface is 5% below the warning threshold percentage of the allowed limit, after having exceeded the maximum percentage threshold of the allowed limit.
Effect	None

10.35 vxlanInterfaceBridgeTableMulticastDestinationsLimitLowered

Table 112: vxlanInterfaceBridgeTableMulticastDestinationsLimitLowered properties

Property name	Value
Application name	bridgetable
Event name	vxlanInterfaceBridgeTableMulticastDestinationsLimitLowered
Default severity	notice
Message format string	The number of Vxlan Multicast Destinations in the bridge table for the vxlan-interface *tunnel-interface*.*vxlan-interface* is now below the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Vxlan Multicast Destinations in a vxlan-interface goes below the allowed limit, after being above the allowed limit
Effect	New Vxlan Multicast Destinations can be added to the vxlan-interface.

10.36 vxlanInterfaceBridgeTableMulticastDestinationsLimitReached

Table 113: vxlanInterfaceBridgeTableMulticastDestinationsLimitReached properties

Property name	Value
Application name	bridgetable
Event name	vxlanInterfaceBridgeTableMulticastDestinationsLimitReached
Default severity	warning
Message format string	The number of Vxlan Multicast Destinations in the bridge table for the vxlan-interface *tunnel-interface*.*vxlan-interface* is at the allowed limit of *maximum-entries*.
Cause	This event is generated when the number of Vxlan Multicast Destinations in a vxlan-interface is at the allowed limit.
Effect	New Vxlan Multicast Destinations cannot be added to the vxlan-interface.

11 chassis

11.1 platformDatapathResourceHighUtilization

Table 114: platformDatapathResourceHighUtilization properties

Property name	Value
Application name	chassis
Event name	platformDatapathResourceHighUtilization
Default severity	warning
Message format string	The datapath resource called *resource-name* has reached *threshold*% or more utilization on linecard *linecard*, forwarding complex *forwarding-complex*
Cause	This event is generated when the utilization of a datapath resource has increased to a level that may warrant concern if further resources are consumed
Effect	None

11.2 platformDatapathResourceHighUtilizationLowered

Table 115: platformDatapathResourceHighUtilizationLowered properties

Property name	Value
Application name	chassis
Event name	platformDatapathResourceHighUtilizationLowered
Default severity	notice
Message format string	The datapath resource called *resource-name* has decreased back to *threshold*% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*
Cause	This event is generated when the utilization of a datapath resource has decreased to a level that may no longer warrant concern
Effect	None

11.3 platformDatapathResourceLimitCleared

Table 116: platformDatapathResourceLimitCleared properties

Property name	Value
Application name	chassis
Event name	platformDatapathResourceLimitCleared
Default severity	notice
Message format string	The datapath resource called *resource-name* has decreased from 100% utilization back to 95% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*
Cause	This event is generated when the utilization of a datapath resource has decreased to a level such that resource exhaustion is no longer imminent
Effect	None

11.4 platformDatapathResourceLimitReached

Table 117: platformDatapathResourceLimitReached properties

Property name	Value
Application name	chassis
Event name	platformDatapathResourceLimitReached
Default severity	warning
Message format string	The datapath resource called *resource-name* has reached 100% utilization on linecard *linecard*, forwarding complex *forwarding-complex*
Cause	This event is generated when the utilization of a datapath resource has exhausted the resource
Effect	None

11.5 platformMtuHighUtilization

Table 118: platformMtuHighUtilization properties

Property name	Value
Application name	chassis
Event name	platformMtuHighUtilization
Default severity	warning
Message format string	The MTU resource called *resource-name* has reached *threshold*% or more utilization on linecard *linecard*, forwarding complex *forwarding-complex*. Only *free-entries* entries are remaining.
Cause	This event is generated when the utilization of an MTU resource has increased to a level that may warrant concern if further resources are consumed
Effect	None

11.6 platformMtuHighUtilizationLowered

Table 119: platformMtuHighUtilizationLowered properties

Property name	Value
Application name	chassis
Event name	platformMtuHighUtilizationLowered
Default severity	notice
Message format string	The MTU resource called *resource-name* has decreased back to *threshold*% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*.
Cause	This event is generated when the utilization of an MTU resource has decreased to a level that may no longer warrant concern
Effect	None

11.7 platformPipelineResourceHighUtilization

Table 120: platformPipelineResourceHighUtilization properties

Property name	Value
Application name	chassis
Event name	platformPipelineResourceHighUtilization
Default severity	warning
Message format string	The pipeline resource called *resource-name* has reached *threshold*% or more utilization on linecard *linecard*, forwarding complex *forwarding-complex*, pipeline *pipeline*
Cause	This event is generated when the utilization of a pipeline resource has increased to a level that may warrant concern if futher resources are consumed
Effect	None

11.8 platformPipelineResourceHighUtilizationLowered

Table 121: platformPipelineResourceHighUtilizationLowered properties

Property name	Value
Application name	chassis
Event name	platformPipelineResourceHighUtilizationLowered
Default severity	notice
Message format string	The pipeline resource called *resource-name* has decreased back to *threshold*% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*, pipeline *pipeline*
Cause	This event is generated when the utilization of a pipeline resource has decreased to a level that may no longer warrant concern
Effect	None

11.9 platformPipelineResourceLimitCleared

Table 122: platformPipelineResourceLimitCleared properties

Property name	Value
Application name	chassis
Event name	platformPipelineResourceLimitCleared
Default severity	notice
Message format string	The pipeline resource called *resource-name* has decreased from 100% utilization back to 95% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*, *pipeline*
Cause	This event is generated when the utilization of a pipeline resource has decreased to a level such that resource exhaustion is no longer imminent
Effect	None

11.10 platformPipelineResourceLimitReached

Table 123: platformPipelineResourceLimitReached properties

Property name	Value
Application name	chassis
Event name	platformPipelineResourceLimitReached
Default severity	warning
Message format string	The pipeline resource called *resource-name* has reached 100% utilization on linecard *linecard*, forwarding complex *forwarding-complex*, *pipeline*
Cause	This event is generated when the utilization of a pipeline resource has exhausted the resource
Effect	None

11.11 portDown

Table 124: portDown properties

Property name	Value
Application name	chassis
Event name	portDown
Default severity	warning
Message format string	Interface *interface_name* is now down for reason: *oper_down_reason*
Cause	The interface has transitioned from the up state to the down state
Effect	The interface is now down

11.12 portUp

Table 125: portUp properties

Property name	Value
Application name	chassis
Event name	portUp
Default severity	notice
Message format string	Interface *interface_name* is now up
Cause	The interface has transitioned from the down state to the up state
Effect	The interface is now up

11.13 secureBootDisabled

Table 126: secureBootDisabled properties

Property name	Value
Application name	chassis
Event name	secureBootDisabled
Default severity	warning
Message format string	Control module *control* booted with Secure Boot Disabled

Property name	Value
Cause	The control module booted with Secure Boot disabled
Effect	Boot software is not subject to signature verification

11.14 secureBootEnabled

Table 127: secureBootEnabled properties

Property name	Value
Application name	chassis
Event name	secureBootEnabled
Default severity	notice
Message format string	Control module *control* booted with Secure Boot Enabled
Cause	The control module booted with Secure Boot Enabled
Effect	Boot software is subject to signature verification

11.15 subinterfaceDown

Table 128: subinterfaceDown properties

Property name	Value
Application name	chassis
Event name	subinterfaceDown
Default severity	warning
Message format string	The subinterface *subinterface_name* is now down for reason: *oper_down_reason*
Cause	This event is generated when the subinterface has transitioned from the up state to the down state
Effect	The subinterface is now down

11.16 subinterfaceUp

Table 129: subinterfaceUp properties

Property name	Value
Application name	chassis
Event name	subinterfaceUp
Default severity	notice
Message format string	The subinterface *subinterface_name* is now up
Cause	This event is generated when the subinterface has transitioned from the down state to the up state.
Effect	The subinterface is now up

11.17 transceiverChannelHighInputPowerAlarm

Table 130: transceiverChannelHighInputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighInputPowerAlarm
Default severity	critical
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more
Cause	The input power of the optical channel has increased
Effect	High input power may affect transceiver performance

11.18 transceiverChannelHighInputPowerAlarmClear

Table 131: transceiverChannelHighInputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighInputPowerAlarmClear

Property name	Value
Default severity	informational
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased below *high_ threshold* dBm
Cause	The input power of the optical channel has decreased
Effect	High input power may affect transceiver performance

11.19 transceiverChannelHighInputPowerWarning

Table 132: transceiverChannelHighInputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighInputPowerWarning
Default severity	warning
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased to *high_ threshold* dBm or more
Cause	The input power of the optical channel has increased
Effect	High input power may affect transceiver performance

11.20 transceiverChannelHighInputPowerWarningClear

Table 133: transceiverChannelHighInputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighInputPowerWarningClear
Default severity	informational
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased below *high_ threshold* dBm
Cause	The input power of the optical channel has decreased

Property name	Value
Effect	High input power may affect transceiver performance

11.21 transceiverChannelHighLaserBiasCurrentAlarm

Table 134: transceiverChannelHighLaserBiasCurrentAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighLaserBiasCurrentAlarm
Default severity	critical
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has increased to *high_threshold* mA or more
Cause	Laser bias increases with temperature and age. Consider lowering the ambient temperature or replacing the laser.
Effect	High laser bias may affect transceiver performance

11.22 transceiverChannelHighLaserBiasCurrentAlarmClear

Table 135: transceiverChannelHighLaserBiasCurrentAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighLaserBiasCurrentAlarmClear
Default severity	informational
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has decreased below *high_threshold* mA
Cause	Laser bias current has decreased
Effect	High laser bias may affect transceiver performance

11.23 transceiverChannelHighLaserBiasCurrentWarning

Table 136: transceiverChannelHighLaserBiasCurrentWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighLaserBiasCurrentWarning
Default severity	warning
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has increased to *high_threshold* mA or more
Cause	Laser bias increases with temperature and age. Consider lowering the ambient temperature or replacing the laser.
Effect	High laser bias may affect transceiver performance

11.24 transceiverChannelHighLaserBiasCurrentWarningClear

Table 137: transceiverChannelHighLaserBiasCurrentWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighLaserBiasCurrentWarningClear
Default severity	informational
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has decreased below *high_threshold* mA
Cause	Laser bias current has decreased
Effect	High laser bias may affect transceiver performance

11.25 transceiverChannelHighOutputPowerAlarm

Table 138: transceiverChannelHighOutputPowerAlarm properties

Property name	Value
Application name	chassis

Property name	Value
Event name	transceiverChannelHighOutputPowerAlarm
Default severity	critical
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more
Cause	The output power of the optical channel has increased
Effect	High output power may affect transceiver performance

11.26 transceiverChannelHighOutputPowerAlarmClear

Table 139: transceiverChannelHighOutputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighOutputPowerAlarmClear
Default severity	informational
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased below *high_threshold* dBm
Cause	The output power of the optical channel has decreased
Effect	High output power may affect transceiver performance

11.27 transceiverChannelHighOutputPowerWarning

Table 140: transceiverChannelHighOutputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighOutputPowerWarning
Default severity	warning
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more

Property name	Value
Cause	The output power of the optical channel has increased
Effect	High output power may affect transceiver performance

11.28 transceiverChannelHighOutputPowerWarningClear

Table 141: transceiverChannelHighOutputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighOutputPowerWarningClear
Default severity	informational
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased below *high_threshold* dBm
Cause	The output power of the optical channel has decreased
Effect	High output power may affect transceiver performance

11.29 transceiverChannelLowInputPowerAlarm

Table 142: transceiverChannelLowInputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowInputPowerAlarm
Default severity	critical
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The input power of the optical channel has decreased
Effect	Low input power may affect transceiver performance

11.30 transceiverChannelLowInputPowerAlarmClear

Table 143: transceiverChannelLowInputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowInputPowerAlarmClear
Default severity	informational
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The input power of the optical channel has increased
Effect	Low input power may affect transceiver performance

11.31 transceiverChannelLowInputPowerWarning

Table 144: transceiverChannelLowInputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowInputPowerWarning
Default severity	warning
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The input power of the optical channel has decreased
Effect	Low input power may affect transceiver performance

11.32 transceiverChannelLowInputPowerWarningClear

Table 145: transceiverChannelLowInputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowInputPowerWarningClear

Property name	Value
Default severity	informational
Message format string	The input power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The input power of the optical channel has increased
Effect	Low input power may affect transceiver performance

11.33 transceiverChannelLowLaserBiasCurrentAlarm

Table 146: transceiverChannelLowLaserBiasCurrentAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowLaserBiasCurrentAlarm
Default severity	critical
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has decreased to *low_threshold* mA or less
Cause	The laser bias current of the optical channel has decreased
Effect	Low laser bias current may affect transceiver performance

11.34 transceiverChannelLowLaserBiasCurrentAlarmClear

Table 147: transceiverChannelLowLaserBiasCurrentAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowLaserBiasCurrentAlarmClear
Default severity	informational
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has increased above *low_threshold* mA
Cause	The laser bias current of the optical channel has increased

Property name	Value
Effect	Low laser bias current may affect transceiver performance

11.35 transceiverChannelLowLaserBiasCurrentWarning

Table 148: transceiverChannelLowLaserBiasCurrentWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowLaserBiasCurrentWarning
Default severity	warning
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has decreased to *low_threshold* mA or less
Cause	The laser bias current of the optical channel has decreased
Effect	Low laser bias current may affect transceiver performance

11.36 transceiverChannelLowLaserBiasCurrentWarningClear

Table 149: transceiverChannelLowLaserBiasCurrentWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowLaserBiasCurrentWarningClear
Default severity	informational
Message format string	The laser bias current supplied to channel *channel_num* of the transceiver associated with interface *interface_name* has increased above *low_threshold* mA
Cause	The laser bias current of the optical channel has increased
Effect	Low laser bias current may affect transceiver performance

11.37 transceiverChannelLowOutputPowerAlarm

Table 150: transceiverChannelLowOutputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowOutputPowerAlarm
Default severity	critical
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The output power of the optical channel has decreased
Effect	Low output power may affect transceiver performance

11.38 transceiverChannelLowOutputPowerAlarmClear

Table 151: transceiverChannelLowOutputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowOutputPowerAlarmClear
Default severity	informational
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The output power of the optical channel has increased
Effect	Low output power may affect transceiver performance

11.39 transceiverChannelLowOutputPowerWarning

Table 152: transceiverChannelLowOutputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowOutputPowerWarning

Property name	Value
Default severity	warning
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The output power of the optical channel has decreased
Effect	Low output power may affect transceiver performance

11.40 transceiverChannelLowOutputPowerWarningClear

Table 153: transceiverChannelLowOutputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelLowOutputPowerWarningClear
Default severity	informational
Message format string	The output power measured for channel *channel_num* of the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The output power of the optical channel has increased
Effect	Low output power may affect transceiver performance

11.41 transceiverHighInputPowerAlarm

Table 154: transceiverHighInputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverHighInputPowerAlarm
Default severity	critical
Message format string	The input power measured for the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more
Cause	The input power of the optics has increased

Property name	Value
Effect	High input power may affect transceiver performance

11.42 transceiverHighInputPowerAlarmClear

Table 155: transceiverHighInputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverHighInputPowerAlarmClear
Default severity	informational
Message format string	The input power measured for the transceiver associated with interface *interface_name* has decreased below *high_threshold* dBm
Cause	The input power of the optics has decreased
Effect	High input power may affect transceiver performance

11.43 transceiverHighInputPowerWarning

Table 156: transceiverHighInputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverHighInputPowerWarning
Default severity	warning
Message format string	The input power measured for the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more
Cause	The input power of the optics has increased
Effect	High input power may affect transceiver performance

11.44 transceiverHighInputPowerWarningClear

Table 157: transceiverHighInputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverHighInputPowerWarningClear
Default severity	informational
Message format string	The input power measured for the transceiver associated with interface *interface_name* has decreased below *high_threshold* dBm
Cause	The input power of the opticsl has decreased
Effect	High input power may affect transceiver performance

11.45 transceiverHighLaserBiasCurrentAlarm

Table 158: transceiverHighLaserBiasCurrentAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverHighLaserBiasCurrentAlarm
Default severity	critical
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has increased to *high_threshold* mA or more
Cause	Laser bias increases with temperature and age. Consider lowering the ambient temperature or replacing the laser.
Effect	High laser bias may affect transceiver performance

11.46 transceiverHighLaserBiasCurrentAlarmClear

Table 159: transceiverHighLaserBiasCurrentAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverHighLaserBiasCurrentAlarmClear

Property name	Value
Default severity	informational
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has decreased below *high_threshold* mA
Cause	Laser bias current has decreased
Effect	High laser bias may affect transceiver performance

11.47 transceiverHighLaserBiasCurrentWarning

Table 160: transceiverHighLaserBiasCurrentWarning properties

Property name	Value
Application name	chassis
Event name	transceiverHighLaserBiasCurrentWarning
Default severity	warning
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has increased to *high_threshold* mA or more
Cause	Laser bias increases with temperature and age. Consider lowering the ambient temperature or replacing the laser.
Effect	High laser bias may affect transceiver performance

11.48 transceiverHighLaserBiasCurrentWarningClear

Table 161: transceiverHighLaserBiasCurrentWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverHighLaserBiasCurrentWarningClear
Default severity	informational
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has decreased below *high_threshold* mA
Cause	Laser bias current has decreased
Effect	High laser bias may affect transceiver performance

11.49 transceiverHighOutputPowerAlarm

Table 162: transceiverHighOutputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverHighOutputPowerAlarm
Default severity	critical
Message format string	The output power measured for the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more
Cause	The output power of the optics has increased
Effect	High output power may affect transceiver performance

11.50 transceiverHighOutputPowerAlarmClear

Table 163: transceiverHighOutputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverHighOutputPowerAlarmClear
Default severity	informational
Message format string	The output power measured for the transceiver associated with interface *interface_name* has decreased below *high_threshold* dBm
Cause	The output power of the optics has decreased
Effect	High output power may affect transceiver performance

11.51 transceiverHighOutputPowerWarning

Table 164: transceiverHighOutputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverHighOutputPowerWarning

Property name	Value
Default severity	warning
Message format string	The output power measured for the transceiver associated with interface *interface_name* has increased to *high_threshold* dBm or more
Cause	The output power of the optics has increased
Effect	High output power may affect transceiver performance

11.52 transceiverHighOutputPowerWarningClear

Table 165: transceiverHighOutputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverHighOutputPowerWarningClear
Default severity	informational
Message format string	The output power measured for the transceiver associated with interface *interface_name* has decreased below *high_threshold* dBm
Cause	The output power of the optics has decreased
Effect	High output power may affect transceiver performance

11.53 transceiverLowInputPowerAlarm

Table 166: transceiverLowInputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverLowInputPowerAlarm
Default severity	critical
Message format string	The input power measured for the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The input power of the optics has decreased
Effect	Low input power may affect transceiver performance

11.54 transceiverLowInputPowerAlarmClear

Table 167: transceiverLowInputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowInputPowerAlarmClear
Default severity	informational
Message format string	The input power measured for the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The input power of the optics has increased
Effect	Low input power may affect transceiver performance

11.55 transceiverLowInputPowerWarning

Table 168: transceiverLowInputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverLowInputPowerWarning
Default severity	warning
Message format string	The input power measured for the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The input power of the optics has decreased
Effect	Low input power may affect transceiver performance

11.56 transceiverLowInputPowerWarningClear

Table 169: transceiverLowInputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowInputPowerWarningClear

Property name	Value
Default severity	informational
Message format string	The input power measured for the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The input power of the optics has increased
Effect	Low input power may affect transceiver performance

11.57 transceiverLowLaserBiasCurrentAlarm

Table 170: transceiverLowLaserBiasCurrentAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverLowLaserBiasCurrentAlarm
Default severity	critical
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has decreased to *low_threshold* mA or less
Cause	The laser bias current of the optics has decreased
Effect	Low laser bias current may affect transceiver performance

11.58 transceiverLowLaserBiasCurrentAlarmClear

Table 171: transceiverLowLaserBiasCurrentAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowLaserBiasCurrentAlarmClear
Default severity	informational
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has increased above *low_threshold* mA
Cause	The laser bias current of the optics has increased
Effect	Low laser bias current may affect transceiver performance

11.59 transceiverLowLaserBiasCurrentWarning

Table 172: transceiverLowLaserBiasCurrentWarning properties

Property name	Value
Application name	chassis
Event name	transceiverLowLaserBiasCurrentWarning
Default severity	warning
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has decreased to *low_threshold* mA or less
Cause	The laser bias current of the optics has decreased
Effect	Low laser bias current may affect transceiver performance

11.60 transceiverLowLaserBiasCurrentWarningClear

Table 173: transceiverLowLaserBiasCurrentWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowLaserBiasCurrentWarningClear
Default severity	informational
Message format string	The laser bias current supplied to the transceiver associated with interface *interface_name* has increased above *low_threshold* mA
Cause	The laser bias current of the optics has increased
Effect	Low laser bias current may affect transceiver performance

11.61 transceiverLowOutputPowerAlarm

Table 174: transceiverLowOutputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverLowOutputPowerAlarm

Property name	Value
Default severity	critical
Message format string	The output power measured for the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The output power of the optics has decreased
Effect	Low output power may affect transceiver performance

11.62 transceiverLowOutputPowerAlarmClear

Table 175: transceiverLowOutputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowOutputPowerAlarmClear
Default severity	informational
Message format string	The output power measured for the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The output power of the optics has increased
Effect	Low output power may affect transceiver performance

11.63 transceiverLowOutputPowerWarning

Table 176: transceiverLowOutputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverLowOutputPowerWarning
Default severity	warning
Message format string	The output power measured for the transceiver associated with interface *interface_name* has decreased to *low_threshold* dBm or less
Cause	The output power of the optics has decreased
Effect	Low output power may affect transceiver performance

11.64 transceiverLowOutputPowerWarningClear

Table 177: transceiverLowOutputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowOutputPowerWarningClear
Default severity	informational
Message format string	The output power measured for the transceiver associated with interface *interface_name* has increased above *low_threshold* dBm
Cause	The output power of the optics has increased
Effect	Low output power may affect transceiver performance

11.65 transceiverModuleDown

Table 178: transceiverModuleDown properties

Property name	Value
Application name	chassis
Event name	transceiverModuleDown
Default severity	warning
Message format string	The transceiver associated with the interface *interface_name* is now down
Cause	The transceiver oper-state has transitioned from the up state to any lower state
Effect	The transceiver is not operational

11.66 transceiverModuleHighTemperatureAlarm

Table 179: transceiverModuleHighTemperatureAlarm properties

Property name	Value
Application name	chassis

Property name	Value
Event name	transceiverModuleHighTemperatureAlarm
Default severity	critical
Message format string	The temperature of the transceiver associated with the interface *interface_name* has increased to *high_threshold* degrees C or more
Cause	The temperature of the transceiver module has increased
Effect	High temperatures may affect transceiver performance

11.67 transceiverModuleHighTemperatureAlarmClear

Table 180: transceiverModuleHighTemperatureAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighTemperatureAlarmClear
Default severity	informational
Message format string	The temperature of the transceiver associated with the interface *interface_name* has decreased below *high_threshold* degrees C
Cause	The temperature of the transceiver module has decreased
Effect	High temperatures may affect transceiver performance

11.68 transceiverModuleHighTemperatureWarning

Table 181: transceiverModuleHighTemperatureWarning properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighTemperatureWarning
Default severity	warning
Message format string	The temperature of the transceiver associated with the interface *interface_name* has increased to *high_threshold* degrees C or more
Cause	The temperature of the transceiver module has increased

Property name	Value
Effect	High temperatures may affect transceiver performance

11.69 transceiverModuleHighTemperatureWarningClear

Table 182: transceiverModuleHighTemperatureWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighTemperatureWarningClear
Default severity	informational
Message format string	The temperature of the transceiver associated with the interface *interface_name* has decreased below *high_threshold* degrees C
Cause	The temperature of the transceiver module has decreased
Effect	High temperatures may affect transceiver performance

11.70 transceiverModuleHighVoltageAlarm

Table 183: transceiverModuleHighVoltageAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighVoltageAlarm
Default severity	critical
Message format string	The voltage of the transceiver associated with the interface *interface_name* has increased to *high_threshold* Volts or more
Cause	The voltage supplied to the transceiver module has increased
Effect	High voltages may affect transceiver performance

11.71 transceiverModuleHighVoltageAlarmClear

Table 184: transceiverModuleHighVoltageAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighVoltageAlarmClear
Default severity	informational
Message format string	The voltage of the transceiver associated with the interface *interface_name* has decreased below *high_threshold* Volts
Cause	The voltage supplied to the transceiver module has decreased
Effect	High voltages may affect transceiver performance

11.72 transceiverModuleHighVoltageWarning

Table 185: transceiverModuleHighVoltageWarning properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighVoltageWarning
Default severity	warning
Message format string	The voltage of the transceiver associated with the interface *interface_name* has increased to *high_threshold* Volts or more
Cause	The voltage supplied to the transceiver module has increased
Effect	High voltages may affect transceiver performance

11.73 transceiverModuleHighVoltageWarningClear

Table 186: transceiverModuleHighVoltageWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighVoltageWarningClear
Default severity	informational

Property name	Value
Message format string	The voltage of the transceiver associated with the interface *interface_name* has decreased below *high_threshold* Volts
Cause	The voltage supplied to the transceiver module has decreased
Effect	High voltages may affect transceiver performance

11.74 transceiverModuleLowTemperatureAlarm

Table 187: transceiverModuleLowTemperatureAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowTemperatureAlarm
Default severity	critical
Message format string	The temperature of the transceiver associated with the interface *interface_name* has decreased to *low_threshold* degrees C or less
Cause	The temperature of the transceiver module has decreased
Effect	Low temperatures may affect transceiver performance

11.75 transceiverModuleLowTemperatureAlarmClear

Table 188: transceiverModuleLowTemperatureAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowTemperatureAlarmClear
Default severity	informational
Message format string	The temperature of the transceiver associated with the interface *interface_name* has increased above *low_threshold* degrees C
Cause	The temperature of the transceiver module has increased
Effect	Low temperatures may affect transceiver performance

11.76 transceiverModuleLowTemperatureWarning

Table 189: transceiverModuleLowTemperatureWarning properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowTemperatureWarning
Default severity	warning
Message format string	The temperature of the transceiver associated with the interface *interface_name* has decreased to *low_threshold* degrees C or less
Cause	The temperature of the transceiver module has decreased
Effect	Low temperatures may affect transceiver performance

11.77 transceiverModuleLowTemperatureWarningClear

Table 190: transceiverModuleLowTemperatureWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowTemperatureWarningClear
Default severity	informational
Message format string	The temperature of the transceiver associated with the interface *interface_name* has increased above *low_threshold* degrees C
Cause	The temperature of the transceiver module has increased
Effect	Low temperatures may affect transceiver performance

11.78 transceiverModuleLowVoltageAlarm

Table 191: transceiverModuleLowVoltageAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowVoltageAlarm
Default severity	critical

Property name	Value
Message format string	The voltage of the transceiver associated with the interface *interface_name* has decreased to *low_threshold* Volts or less
Cause	The voltage supplied to the transceiver module has decreased
Effect	Low voltages may affect transceiver performance

11.79 transceiverModuleLowVoltageAlarmClear

Table 192: transceiverModuleLowVoltageAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowVoltageAlarmClear
Default severity	informational
Message format string	The voltage of the transceiver associated with the interface *interface_name* has increased above *low_threshold* Volts
Cause	The voltage supplied to the transceiver module has increased
Effect	Low voltages may affect transceiver performance

11.80 transceiverModuleLowVoltageWarning

Table 193: transceiverModuleLowVoltageWarning properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowVoltageWarning
Default severity	warning
Message format string	The voltage of the transceiver associated with the interface *interface_name* has decreased to *low_threshold* Volts or less
Cause	The voltage supplied to the transceiver module has decreased
Effect	Low voltages may affect transceiver performance

11.81 transceiverModuleLowVoltageWarningClear

Table 194: transceiverModuleLowVoltageWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowVoltageWarningClear
Default severity	informational
Message format string	The voltage of the transceiver associated with the interface *interface_name* has increased above *low_threshold* Volts
Cause	The voltage supplied to the transceiver module has increased
Effect	Low voltages may affect transceiver performance

11.82 transceiverModuleUp

Table 195: transceiverModuleUp properties

Property name	Value
Application name	chassis
Event name	transceiverModuleUp
Default severity	notice
Message format string	The transceiver associated with the interface *interface_name* is now up
Cause	The transceiver oper-state has transitioned from any other state to the up state
Effect	The transceiver is now operational

12 debug

12.1 setAllConfigLevels

Table 196: setAllConfigLevels properties

Property name	Value
Application name	debug
Event name	setAllConfigLevels
Default severity	informational
Message format string	App config debug log levels set to: *new_level*.
Cause	Configuration of debug log levels that can be received by program parameter or via idb.
Effect	Sticky levels are losable only to another configuration setting.

12.2 setAllStartupLevels

Table 197: setAllStartupLevels properties

Property name	Value
Application name	debug
Event name	setAllStartupLevels
Default severity	informational
Message format string	App debug startup log levels set to: *new_level* (configuration can override).
Cause	Restrain of logging verbosity internal to some programs
Effect	If configuration is set, and goes away, the startup levels are respected.

12.3 setHighBaselineLogLevels

Table 198: setHighBaselineLogLevels properties

Property name	Value
Application name	debug
Event name	setHighBaselineLogLevels
Default severity	informational
Message format string	Default (startup), and runtime app debug log levels set to: *new_level*. Except for modules: {*configured_list*}
Cause	Boot phase time is up, and verbose messages are suppressed in a beta build with .
Effect	Internal setting to all levels. If module levels are configured, they restore to the setting.

13 dhcp

13.1 dhcp6ClientAddressDeclined

Table 199: dhcp6ClientAddressDeclined properties

Property name	Value
Application name	dhcp
Event name	dhcp6ClientAddressDeclined
Default severity	notice
Message format string	DHCPv6 client running on *subinterface_name* was given a duplicate IPv6 address by the DHCP server *server_ip*
Cause	The DHCP server assigned an IPv6 address that is already in use on the same subnet
Effect	The subinterface will try to acquire a new IPv6 address

13.2 dhcp6ClientIpv6AddressValidLifetimeExpired

Table 200: dhcp6ClientIpv6AddressValidLifetimeExpired properties

Property name	Value
Application name	dhcp
Event name	dhcp6ClientIpv6AddressValidLifetimeExpired
Default severity	warning
Message format string	The IPv6 address *assigned_ip* obtained by the DHCPv6 client running on *subinterface_name* has become invalid
Cause	The DHCPv6 client was not successful in renewing or rebinding the IA_NA lease before the valid lifetime of the IPv6 address expired
Effect	The subinterface has no DHCP-assigned IPv6 address

13.3 dhcp6ClientRebindAttempted

Table 201: dhcp6ClientRebindAttempted properties

Property name	Value
Application name	dhcp
Event name	dhcp6ClientRebindAttempted
Default severity	informational
Message format string	DHCPv6 client running on *subinterface_name* is attempting to rebind its IA_NA lease for the IPv6 address *requested_ip*
Cause	The DHCPv6 client could not renew its assigned IPv6 address before the timer T2 expired
Effect	The IPv6 address may become deprecated and then invalid if the rebind is not successful

13.4 dhcp6ClientReconfigureMsgDropped

Table 202: dhcp6ClientReconfigureMsgDropped properties

Property name	Value
Application name	dhcp
Event name	dhcp6ClientReconfigureMsgDropped
Default severity	notice
Message format string	The DHCPv6 client running on *subinterface_name* dropped a RECONFIGURE message received from the server *server_ip*
Cause	The DHCPv6 client received a message that it was not supposed to receive (because it did not include a Reconfigure Accept option in its SOLICIT msg)
Effect	None

13.5 dhcp6ClientRenewSuccess

Table 203: dhcp6ClientRenewSuccess properties

Property name	Value
Application name	dhcp
Event name	dhcp6ClientRenewSuccess
Default severity	informational
Message format string	DHCPv6 client running on *subinterface_name* successfully renewed the IPv6 address *requested_ip* for a new lease duration of *new_lease_time* seconds from server *server_ip*
Cause	The DHCPv6 client received a success REPLY in response to its RENEW
Effect	The subinterface remains operational with its existing DHCP-assigned IPv6 address

13.6 dhcpClientAddressDeclined

Table 204: dhcpClientAddressDeclined properties

Property name	Value
Application name	dhcp
Event name	dhcpClientAddressDeclined
Default severity	notice
Message format string	DHCP client running on *subinterface_name* was given a duplicate IPv4 address by the DHCP server *server_ip*
Cause	The DHCP server assigned an IPv4 address that is already in use on the same subnet
Effect	The subinterface will try to acquire a new IPv4 address after a 10s delay

13.7 dhcpClientLeaseExpired

Table 205: dhcpClientLeaseExpired properties

Property name	Value
Application name	dhcp
Event name	dhcpClientLeaseExpired
Default severity	warning
Message format string	The DHCP lease for address *assigned_ip* obtained by the DHCP client running on *subinterface_name* and obtained from server *server_ip* has expired
Cause	The DHCP client was not successful in renewing or rebinding the lease
Effect	The subinterface has no DHCP-assigned IPv4 address

13.8 dhcpClientRebindAttempted

Table 206: dhcpClientRebindAttempted properties

Property name	Value
Application name	dhcp
Event name	dhcpClientRebindAttempted
Default severity	informational
Message format string	DHCP client running on *subinterface_name* is attempting to rebind its lease for the IP address *requested_ip*
Cause	The DHCP client could not renew its assigned IPv4 address before the timer T2 expired
Effect	The lease may expire if the rebind is not successful

13.9 dhcpClientRenewSuccess

Table 207: dhcpClientRenewSuccess properties

Property name	Value
Application name	dhcp
Event name	dhcpClientRenewSuccess

Property name	Value
Default severity	informational
Message format string	DHCP client running on *subinterface_name* successfully renewed the IP address *requested_ip* for a new lease duration of *new_lease_time* seconds from server *server_ip*
Cause	The DHCP client received a DHCPACK response to its DHCPREQUEST
Effect	The subinterface remains operational with its existing DHCP-assigned IPv4 address

13.10 dhcpv4RelayAdminDisable

Table 208: dhcpv4RelayAdminDisable properties

Property name	Value
Application name	dhcp
Event name	dhcpv4RelayAdminDisable
Default severity	warning
Message format string	DHCPv4 Relay on sub-interface *subinterface_name* has changed to administrative disable state
Cause	The DHCPv4 Relay admin state has changed from enable to disable due to configuration change
Effect	The DHCPv4 Relay admin state is disable on the mentioned sub-interface

13.11 dhcpv4RelayAdminEnable

Table 209: dhcpv4RelayAdminEnable properties

Property name	Value
Application name	dhcp
Event name	dhcpv4RelayAdminEnable
Default severity	warning
Message format string	DHCPv4 Relay on sub-interface *subinterface_name* has changed to administrative enable state

Property name	Value
Cause	The DHCPv4 Relay admin state has changed from disable to enable due to configuration change
Effect	The DHCPv4 Relay admin state is enable on the mentioned sub-interface

13.12 dhcpv4RelayAllDhcpv4ServersUnreachable

Table 210: dhcpv4RelayAllDhcpv4ServersUnreachable properties

Property name	Value
Application name	dhcp
Event name	dhcpv4RelayAllDhcpv4ServersUnreachable
Default severity	critical
Message format string	All DHCPv4 Servers *dhcpv4_server_list* configured under DHCPv4 Relay on sub-interface *subinterface_name* are unreachable for network instance *network_instance*
Cause	All The DHCPv4 Servers configured under DHCPv4 Relay are unreachable
Effect	The DHCPv4 Relay oper state is down on the mentioned sub-interface

13.13 dhcpv4RelayOperDown

Table 211: dhcpv4RelayOperDown properties

Property name	Value
Application name	dhcp
Event name	dhcpv4RelayOperDown
Default severity	critical
Message format string	DHCPv4 Relay on sub-interface *subinterface_name* has changed to operational down state
Cause	The DHCPv4 Relay oper state has changed from up to down
Effect	The DHCPv4 Relay oper state is down on the mentioned sub-interface

13.14 dhcpv4RelayOperUp

Table 212: dhcpv4RelayOperUp properties

Property name	Value
Application name	dhcp
Event name	dhcpv4RelayOperUp
Default severity	warning
Message format string	DHCPv4 Relay on sub-interface *subinterface_name* has changed to operational up state
Cause	The DHCPv4 Relay oper state has changed from down to up
Effect	The DHCPv4 Relay oper state is up on the mentioned sub-interface

13.15 dhcpv6RelayAdminDisable

Table 213: dhcpv6RelayAdminDisable properties

Property name	Value
Application name	dhcp
Event name	dhcpv6RelayAdminDisable
Default severity	warning
Message format string	DHCPv6 Relay on sub-interface *subinterface_name* has changed to administrative disable state
Cause	The DHCPv6 Relay admin state has changed from enable to disable due to configuration change
Effect	The DHCPv6 Relay admin state is disable on the mentioned sub-interface

13.16 dhcpv6RelayAdminEnable

Table 214: dhcpv6RelayAdminEnable properties

Property name	Value
Application name	dhcp

Property name	Value
Event name	dhcpv6RelayAdminEnable
Default severity	warning
Message format string	DHCPv6 Relay on sub-interface *subinterface_name* has changed to administrative enable state
Cause	The DHCPv6 Relay admin state has changed from disable to enable due to configuration change
Effect	The DHCPv6 Relay admin state is enable on the mentioned sub-interface

13.17 dhcpv6RelayAllDhcpv6ServersUnreachable

Table 215: dhcpv6RelayAllDhcpv6ServersUnreachable properties

Property name	Value
Application name	dhcp
Event name	dhcpv6RelayAllDhcpv6ServersUnreachable
Default severity	critical
Message format string	All DHCPv6 Servers *dhcpv6_server_list* configured under DHCPv6 Relay on sub-interface *subinterface_name* are unreachable for network instance *network_instance*
Cause	All The DHCPv6 Servers configured under DHCPv6 Relay are unreachable
Effect	The DHCPv6 Relay oper state is down on the mentioned sub-interface

13.18 dhcpv6RelayOperDown

Table 216: dhcpv6RelayOperDown properties

Property name	Value
Application name	dhcp
Event name	dhcpv6RelayOperDown
Default severity	critical

Property name	Value
Message format string	DHCPv6 Relay on sub-interface *subinterface_name* has changed to operational down state
Cause	The DHCPv6 Relay oper state has changed from up to down
Effect	The DHCPv6 Relay oper state is down on the mentioned sub-interface

13.19 dhcpv6RelayOperUp

Table 217: dhcpv6RelayOperUp properties

Property name	Value
Application name	dhcp
Event name	dhcpv6RelayOperUp
Default severity	warning
Message format string	DHCPv6 Relay on sub-interface *subinterface_name* has changed to operational up state
Cause	The DHCPv6 Relay oper state has changed from down to up
Effect	The DHCPv6 Relay oper state is up on the mentioned sub-interface

13.20 giAddressMismatch

Table 218: giAddressMismatch properties

Property name	Value
Application name	dhcp
Event name	giAddressMismatch
Default severity	critical
Message format string	Gi-Address for DHCPv4 Relay on sub-interface *subinterface_name* does not match any of the configured IPv4 addresses under sub-interface
Cause	The gi-address for DHCPv4 Relay does not match any of the configured IPv4 addresses under sub-interface
Effect	The DHCPv4 Relay oper state is down on the mentioned sub-interface

13.21 sourceAddressMismatch

Table 219: sourceAddressMismatch properties

Property name	Value
Application name	dhcp
Event name	sourceAddressMismatch
Default severity	critical
Message format string	source-address for DHCPv6 Relay on sub-interface *subinterface_name* does not match any of the configured IPv6 addresses under sub-interface
Cause	The source-address for DHCPv6 Relay does not match any of the configured IPv6 addresses under sub-interface
Effect	The DHCPv6 Relay oper state is down on the mentioned sub-interface

14 ethcfm

14.1 ClearErrorCcm

Table 220: ClearErrorCcm properties

Property name	Value
Application name	ethcfm
Event name	ClearErrorCcm
Default severity	notice
Message format string	ETHCFM: The condition of ERROR-CCM on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID, correct MEP ID, correct period.
Effect	The MEP has cleared a defect.

14.2 ClearLOC

Table 221: ClearLOC properties

Property name	Value
Application name	ethcfm
Event name	ClearLOC
Default severity	notice
Message format string	ETHCFM: The condition of loss of continuity (LOC) on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives CCM frames from a peer MEP during an interval equal to 3.5 times the CCM transmission period.
Effect	The MEP has cleared a defect.

14.3 ClearMacStatus

Table 222: ClearMacStatus properties

Property name	Value
Application name	ethcfm
Event name	ClearMacStatus
Default severity	notice
Message format string	ETHCFM: The condition of MAC-STATUS on MEP *domain-id*/ *association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives CCM frames from a peer MEP during an interval equal to 3.5 times the CCM transmission period.
Effect	The MEP has cleared a defect.

14.4 ClearMMG

Table 223: ClearMMG properties

Property name	Value
Application name	ethcfm
Event name	ClearMMG
Default severity	notice
Message format string	ETHCFM: The condition of mismerge (MMG) on MEP *domain-id*/ *association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID.
Effect	The MEP has cleared a defect.

14.5 clearOneWayDmTCA

Table 224: clearOneWayDmTCA properties

Property name	Value
Application name	ethcfm

Property name	Value
Event name	clearOneWayDmTCA
Default severity	notice
Message format string	ETHCFM: A TCA is cleared for one-way delay measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*bin-type*/*direction*'.
Cause	This notification is generated when the result of performance monitoring of an one-way delay measurement has fallen below the clear-threshold.
Effect	The alarm is cleared.

14.6 ClearRDI

Table 225: ClearRDI properties

Property name	Value
Application name	ethcfm
Event name	ClearRDI
Default severity	notice
Message format string	ETHCFM: The remote defect indication (RDI) condition on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with the RDI field clear.
Effect	The MEP has cleared a defect.

14.7 ClearRemoteCcm

Table 226: ClearRemoteCcm properties

Property name	Value
Application name	ethcfm
Event name	ClearRemoteCcm
Default severity	notice
Message format string	ETHCFM: The condition of REMOTE-CCM on MEP *domain-id*/*association-id*/*mep-id* was cleared.

Property name	Value
Cause	This notification is generated when a MEP receives CCM frames from a peer MEP during an interval equal to 3.5 times the CCM transmission period.
Effect	The MEP has cleared a defect.

14.8 ClearRemoteDefectIndication

Table 227: ClearRemoteDefectIndication properties

Property name	Value
Application name	ethcfm
Event name	ClearRemoteDefectIndication
Default severity	notice
Message format string	ETHCFM: The remote defect indication (RDI) condition on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with the RDI field clear.
Effect	The MEP has cleared a defect.

14.9 clearTwoWayDmTCA

Table 228: clearTwoWayDmTCA properties

Property name	Value
Application name	ethcfm
Event name	clearTwoWayDmTCA
Default severity	notice
Message format string	ETHCFM: A TCA is cleared for two-way delay measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*bin-type*/*direction*'.
Cause	This notification is generated when the result of performance monitoring of a two-way delay measurement has fallen below the clear-threshold.
Effect	The alarm is cleared.

14.10 clearTwoWaySlmAvgflrTCA

Table 229: clearTwoWaySlmAvgflrTCA properties

Property name	Value
Application name	ethcfm
Event name	clearTwoWaySlmAvgflrTCA
Default severity	notice
Message format string	ETHCFM: A TCA is cleared for average flr of two-way synthetic loss measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*direction*'.
Cause	This notification is generated when the average flr of a two-way synthetic loss measurement has fallen below the clear-threshold.
Effect	The alarm is cleared.

14.11 clearTwoWaySlmHliTCA

Table 230: clearTwoWaySlmHliTCA properties

Property name	Value
Application name	ethcfm
Event name	clearTwoWaySlmHliTCA
Default severity	notice
Message format string	ETHCFM: A TCA is cleared for high loss of two-way synthetic loss measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*direction*'.
Cause	This notification is generated when the high loss interval of a two-way synthetic loss measurement has fallen below the clear-threshold.
Effect	The alarm is cleared.

14.12 clearTwoWaySlmUnavailTCA

Table 231: clearTwoWaySlmUnavailTCA properties

Property name	Value
Application name	ethcfm
Event name	clearTwoWaySlmUnavailTCA
Default severity	notice
Message format string	ETHCFM: A TCA is cleared for unavailability of two-way synthetic loss measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*direction*'.
Cause	This notification is generated when the unavailability intervals of a two-way synthetic loss measurement has fallen below the clear-threshold.
Effect	The alarm is cleared.

14.13 ClearUNL

Table 232: ClearUNL properties

Property name	Value
Application name	ethcfm
Event name	ClearUNL
Default severity	notice
Message format string	ETHCFM: The condition of unexpected MEG level (UNL) on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level.
Effect	The MEP has cleared a defect.

14.14 ClearUNM

Table 233: ClearUNM properties

Property name	Value
Application name	ethcfm

Property name	Value
Event name	ClearUNM
Default severity	notice
Message format string	ETHCFM: The condition of unexpected MEP (UNM) on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID, correct MEP ID.
Effect	The MEP has cleared a defect.

14.15 ClearUNP

Table 234: ClearUNP properties

Property name	Value
Application name	ethcfm
Event name	ClearUNP
Default severity	notice
Message format string	ETHCFM: The condition of unexpected period (UNP) on MEP *domain-id*/*association-id*/*mep-id* was cleared.
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID, correct MEP ID, correct period.
Effect	The MEP has cleared a defect.

14.16 ClearXconCcm

Table 235: ClearXconCcm properties

Property name	Value
Application name	ethcfm
Event name	ClearXconCcm
Default severity	notice
Message format string	ETHCFM: The condition of XCON-CCM on MEP *domain-id*/*association-id*/*mep-id* was cleared.

Property name	Value
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level.
Effect	The MEP has cleared a defect.

14.17 linktraceCompleted

Table 236: linktraceCompleted properties

Property name	Value
Application name	ethcfm
Event name	linktraceCompleted
Default severity	notice
Message format string	ETHCFM: A linktrace test from MEP *domain-id*/*association-id*/*mep-id* to the destination address *target* has completed.
Cause	This notification is generated when an on-demand linktrace test was successfully completed.
Effect	The test result is stored in the MEP object.

14.18 loopbackCompleted

Table 237: loopbackCompleted properties

Property name	Value
Application name	ethcfm
Event name	loopbackCompleted
Default severity	notice
Message format string	ETHCFM: A loopback test from MEP *domain-id*/*association-id*/*mep-id* to the destination address *target* has completed.
Cause	This notification is generated when an on-demand loopback test was successfully completed.
Effect	The test result is stored in the MEP object.

14.19 RaiseErrorCcm

Table 238: RaiseErrorCcm properties

Property name	Value
Application name	ethcfm
Event name	RaiseErrorCcm
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of ERROR-CCM.
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID, correct MEP ID, but with a period field value different than its own CCM transmission period.
Effect	The MEP has a defect.

14.20 RaiseLOC

Table 239: RaiseLOC properties

Property name	Value
Application name	ethcfm
Event name	RaiseLOC
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of loss of continuity (LOC).
Cause	This notification is generated when a MEP receives no CCM frames from a peer MEP during an interval equal to 3.5 times the CCM transmission period.
Effect	The MEP has a defect.

14.21 RaiseMacStatus

Table 240: RaiseMacStatus properties

Property name	Value
Application name	ethcfm
Event name	RaiseMacStatus
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of MAC-STATUS.
Cause	This notification is generated when a MEP receives no CCM frames from a peer MEP during an interval equal to 3.5 times the CCM transmission period.
Effect	The MEP has a defect.

14.22 RaiseMMG

Table 241: RaiseMMG properties

Property name	Value
Application name	ethcfm
Event name	RaiseMMG
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of mismerge (MMG).
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level but incorrect MEG ID.
Effect	The MEP has a defect.

14.23 raiseOneWayDmTCA

Table 242: raiseOneWayDmTCA properties

Property name	Value
Application name	ethcfm

Property name	Value
Event name	raiseOneWayDmTCA
Default severity	warning
Message format string	ETHCFM: A TCA is raised for one-way delay measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*bin-type*/*direction*'.
Cause	This notification is generated when the result of performance monitoring of a one-way delay measurement has reached or exceeded the raise-threshold.
Effect	An alarm is raised.

14.24 RaiseRDI

Table 243: RaiseRDI properties

Property name	Value
Application name	ethcfm
Event name	RaiseRDI
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of remote defect indication (RDI).
Cause	This notification is generated when a MEP receives a CCM frame with the RDI field set.
Effect	The MEP has a defect.

14.25 RaiseRemoteCcm

Table 244: RaiseRemoteCcm properties

Property name	Value
Application name	ethcfm
Event name	RaiseRemoteCcm
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of REMOTE-CCM.

Property name	Value
Cause	This notification is generated when a MEP receives no CCM frames from a peer MEP during an interval equal to 3.5 times the CCM transmission period.
Effect	The MEP has a defect.

14.26 RaiseRemoteDefectIndication

Table 245: RaiseRemoteDefectIndication properties

Property name	Value
Application name	ethcfm
Event name	RaiseRemoteDefectIndication
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of remote defect indication (RDI).
Cause	This notification is generated when a MEP receives a CCM frame with the RDI field set.
Effect	The MEP has a defect.

14.27 raiseTwoWayDmTCA

Table 246: raiseTwoWayDmTCA properties

Property name	Value
Application name	ethcfm
Event name	raiseTwoWayDmTCA
Default severity	warning
Message format string	ETHCFM: A TCA is raised for two-way delay measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*bin-type*/*direction*'.
Cause	This notification is generated when the result of performance monitoring of a two-way delay measurement has reached or exceeded the raise-threshold.
Effect	An alarm is raised.

14.28 raiseTwoWaySlmAvgflrTCA

Table 247: raiseTwoWaySlmAvgflrTCA properties

Property name	Value
Application name	ethcfm
Event name	raiseTwoWaySlmAvgflrTCA
Default severity	warning
Message format string	ETHCFM: A TCA is raised for average flr of two-way synthetic loss measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*direction*'.
Cause	This notification is generated when the average flr of a two-way synthetic loss measurement has reached or exceeded the raise-threshold.
Effect	An alarm is raised.

14.29 raiseTwoWaySlmHliTCA

Table 248: raiseTwoWaySlmHliTCA properties

Property name	Value
Application name	ethcfm
Event name	raiseTwoWaySlmHliTCA
Default severity	warning
Message format string	ETHCFM: A TCA is raised for high loss of two-way synthetic loss measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*direction*'.
Cause	This notification is generated when the high loss intervals of a two-way synthetic loss measurement has reached or exceeded the raise-threshold.
Effect	An alarm is raised.

14.30 raiseTwoWaySlmUnavailTCA

Table 249: raiseTwoWaySlmUnavailTCA properties

Property name	Value
Application name	ethcfm
Event name	raiseTwoWaySlmUnavailTCA
Default severity	warning
Message format string	ETHCFM: A TCA is raised for unavailability of two-way synthetic loss measurement PM test ' *domain-id*/*association-id*/*mep-id*/*session-id*/ *mi-type*/*direction*'.
Cause	This notification is generated when the unavailability intervals of a two-way synthetic loss measurement has reached or exceeded the raise-threshold.
Effect	An alarm is raised.

14.31 RaiseUNL

Table 250: RaiseUNL properties

Property name	Value
Application name	ethcfm
Event name	RaiseUNL
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of unexpected MEG level (UNL).
Cause	This notification is generated when a MEP receives a CCM frame with incorrect MEG level.
Effect	The MEP has a defect.

14.32 RaiseUNM

Table 251: RaiseUNM properties

Property name	Value
Application name	ethcfm
Event name	RaiseUNM
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of unexpected MEP (UNM).
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID but with unexpected MEP ID.
Effect	The MEP has a defect.

14.33 RaiseUNP

Table 252: RaiseUNP properties

Property name	Value
Application name	ethcfm
Event name	RaiseUNP
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of unexpected period (UNP).
Cause	This notification is generated when a MEP receives a CCM frame with correct MEG level, correct MEG ID, correct MEP ID, but with a period field value different than its own CCM transmission period.
Effect	The MEP has a defect.

14.34 RaiseXconCcm

Table 253: RaiseXconCcm properties

Property name	Value
Application name	ethcfm

Property name	Value
Event name	RaiseXconCcm
Default severity	warning
Message format string	ETHCFM: MEP *domain-id*/ *association-id*/*mep-id* has a condition of XCON-CCM.
Cause	This notification is generated when a MEP receives a CCM frame with incorrect MEG level.
Effect	The MEP has a defect.

14.35 singleEndedDmmCompleted

Table 254: singleEndedDmmCompleted properties

Property name	Value
Application name	ethcfm
Event name	singleEndedDmmCompleted
Default severity	notice
Message format string	ETHCFM: A single-ended delay measurement test (*test-id*) from MEP *domain-id*/*association-id*/*mep-id* to the destination address *target* has completed.
Cause	This notification is generated when an on-demand single-ended delay measurement test was successfully completed.
Effect	The test result is stored in the MEP object.

14.36 singleEndedSlmCompleted

Table 255: singleEndedSlmCompleted properties

Property name	Value
Application name	ethcfm
Event name	singleEndedSlmCompleted
Default severity	notice

Property name	Value
Message format string	ETHCFM: A single-ended synthetic loss measurement test (*test-id*) from MEP *domain-id*/*association-id*/*mep-id* to the destination address *target* has completed.
Cause	This notification is generated when an on-demand single-ended synthetic loss measurement test was successfully completed.
Effect	The test result is stored in the MEP object.

14.37 TwoWaySlmAvailabilityState

Table 256: TwoWaySlmAvailabilityState properties

Property name	Value
Application name	ethcfm
Event name	TwoWaySlmAvailabilityState
Default severity	notice
Message format string	ETHCFM: The availability state has transited to ' *availability*' in two-way synthetic loss measurement PM test '*domain-id*/ *association-id*/*mep-id*/ *session-id*/*mi-type*/*direction*' at ' *transition-time*'.
Cause	This notification is generated when the availability of a two-way synthetic loss measurement has transited from Available to Unavailable or vice versa.
Effect	The notice is sent.

15 evpn

15.1 ethernetsegmentNetworkInstanceBgpInstanceDfStatusChanged

Table 257: ethernetsegmentNetworkInstanceBgpInstanceDfStatusChanged properties

Property name	Value
Application name	evpn
Event name	ethernetsegmentNetworkInstanceBgpInstanceDfStatusChanged
Default severity	notice
Message format string	BGP-EVPN attachment circuit on ethernet segment *ethernet-segment* on network instance *network-instance* and bgp instance *bgp-instance* is now a *designated-forwarding-status*.
Cause	This event is generated when there is a change in the ethernet segment attachment circuit designated forwarder state.
Effect	The forwarding state of the ethernet segment attachment circuit is changed.

15.2 ethernetsegmentPreferenceOperValueChanged

Table 258: ethernetsegmentPreferenceOperValueChanged properties

Property name	Value
Application name	evpn
Event name	ethernetsegmentPreferenceOperValueChanged
Default severity	notice
Message format string	The Oper DF preference value changed to *oper-preference* and/or the DP value changed to *do-not-preempt* on ethernet-segment *ethernet-segment*
Cause	This event is generated when there is a change in the ethernet segment operational preference value or the do not preempt value.
Effect	The designated forwarder state of the ethernet segment's attachment circuit might change.

15.3 evpnAutoDiscoveryEviRouteAddDroppedDueToUnexpectedEthTag

Table 259: evpnAutoDiscoveryEviRouteAddDroppedDueToUnexpectedEthTag properties

Property name	Value
Application name	evpn
Event name	evpnAutoDiscoveryEviRouteAddDroppedDueToUnexpectedEthTag
Default severity	warning
Message format string	BGP-EVPN Auto Discovery Evi route received with route-distinguisher *route-distinguisher* and ethernet segment identifier *ethernet-segment-id* add on network instance *network-instance* and bgp instance *bgp-instance* is dropped because the Ethernet Tag Identifier *received-ethernet-tag* received in the route, does not match locally configured Ethernet Tag Identifier *local-ethernet-tag* on the bgp-instance
Cause	This event is generated when a received Ethernet Tag Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The designated forwarder election on this ethernet-segment-id for this EVI will be affected. The mac-address's on this ethernet-segment will not be programmed in the bridge-table

15.4 evpnAutoDiscoveryEviRouteWithdrawDroppedDueToUnexpectedEthTag

Table 260: evpnAutoDiscoveryEviRouteWithdrawDroppedDueToUnexpectedEthTag properties

Property name	Value
Application name	evpn
Event name	evpnAutoDiscoveryEviRouteWithdrawDroppedDueToUnexpectedEthTag
Default severity	warning
Message format string	BGP-EVPN Auto Discovery Evi route received with route-distinguisher *route-distinguisher* and ethernet segment identifier *ethernet-segment-id* delete on network instance *network-instance* and bgp instance *bgp-instance* is dropped because the Ethernet Tag Identifier *received-ethernet-tag* received in the route, does not match locally configured Ethernet Tag Identifier *local-ethernet-tag* on the bgp-instance

Property name	Value
Cause	This event is generated when a received Ethernet Tag Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The designated forwarder election on this ethernet-segment-id for this EVI will be affected. The mac-address's on this ethernet-segment if programmed in the bridge-table, will not be deleted or updated

15.5 evpnAutoDiscoveryEviRouteWithdrawnDueToUnexpectedVni

Table 261: evpnAutoDiscoveryEviRouteWithdrawnDueToUnexpectedVni properties

Property name	Value
Application name	evpn
Event name	evpnAutoDiscoveryEviRouteWithdrawnDueToUnexpectedVni
Default severity	warning
Message format string	BGP-EVPN Auto Discovery Evi route received with route-distinguisher *route-distinguisher* and ethernet segment identifier *ethernet-segment-id* on network instance *network-instance* and bgp instance *bgp-instance* is withdrawn because the VXLAN Network Identifier *received-vni* received in the route, does not match locally configured VXLAN Network Identifier *local-vni* on the bgp-instance
Cause	This event is generated when a received VXLAN Network Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The designated forwarder election on this ethernet-segment-id for this EVI will be affected. The mac-address's on this ethernet-segment will not be programmed in the bridge-table

15.6 evpnInclMcastRouteAddDroppedDueToUnexpectedEthTag

Table 262: evpnInclMcastRouteAddDroppedDueToUnexpectedEthTag properties

Property name	Value
Application name	evpn
Event name	evpnInclMcastRouteAddDroppedDueToUnexpectedEthTag
Default severity	warning

Property name	Value
Message format string	BGP-EVPN Inclusive Multicast route received with route-distinguisher *route-distinguisher* and originating IP *originating-ip-address* add on network instance *network-instance* and bgp instance *bgp-instance* is dropped because the Ethernet Tag Identifier *received-ethernet-tag* received in the route, does not match locally configured Ethernet Tag Identifier *local-ethernet-tag* on the bgp-instance
Cause	This event is generated when a received Ethernet Tag Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The Virtual Tunnel End Point for the received VXLAN Network Identifier is not programmed in the multicast flood list of bridge-table

15.7 evpnInclMcastRouteWithdrawDroppedDueToUnexpectedEthTag

Table 263: evpnInclMcastRouteWithdrawDroppedDueToUnexpectedEthTag properties

Property name	Value
Application name	evpn
Event name	evpnInclMcastRouteWithdrawDroppedDueToUnexpectedEthTag
Default severity	warning
Message format string	BGP-EVPN Inclusive Multicast route received with route-distinguisher *route-distinguisher* and originating IP *originating-ip-address* withdraw on network instance *network-instance* and bgp instance *bgp-instance* is dropped because the Ethernet Tag Identifier *received-ethernet-tag* received in the route, does not match locally configured Ethernet Tag Identifier *local-ethernet-tag* on the bgp-instance
Cause	This event is generated when a received Ethernet Tag Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The Virtual Tunnel End Point for the received VXLAN Network Identifier if programmed in the multicast flood list of bridge-table, might not be removed

15.8 evpnInclMcastRouteWithdrawnDueToUnexpectedVni

Table 264: evpnInclMcastRouteWithdrawnDueToUnexpectedVni properties

Property name	Value
Application name	evpn
Event name	evpnInclMcastRouteWithdrawnDueToUnexpectedVni
Default severity	warning
Message format string	BGP-EVPN Inclusive Multicast route received with route-distinguisher *route-distinguisher* and originating IP *originating-ip-address* on network instance *network-instance* and bgp instance *bgp-instance* is withdrawn because the VXLAN Network Identifier *received-vni* received in the route, does not match locally configured VXLAN Network Identifier *local-vni* on the bgp-instance
Cause	This event is generated when a received VXLAN Network Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The Virtual Tunnel End Point for the received VXLAN Network Identifier is not programmed in the multicast flood list of bridge-table

15.9 evpnIpPrefixRouteNotImportedDueToUnexpectedVni

Table 265: evpnIpPrefixRouteNotImportedDueToUnexpectedVni properties

Property name	Value
Application name	evpn
Event name	evpnIpPrefixRouteNotImportedDueToUnexpectedVni
Default severity	warning
Message format string	BGP-EVPN IP-PREFIX *ip-prefix* LENGTH *prefix-length* received with route-distinguisher *route-distinguisher* on network instance *network-instance* and bgp instance *bgp-instance* is not imported because the VXLAN Network Identifier *received-vni* received in the route, does not match the locally configured VXLAN Network Identifier on the bgp-instance
Cause	This event is generated when a received VXLAN Network Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The IP-Prefix is not programmed in the route-table

15.10 evpnIpPrefixRouteWithdrawnDueToNoGwMac

Table 266: evpnIpPrefixRouteWithdrawnDueToNoGwMac properties

Property name	Value
Application name	evpn
Event name	evpnIpPrefixRouteWithdrawnDueToNoGwMac
Default severity	warning
Message format string	BGP-EVPN IP-PREFIX *ip-prefix* LENGTH *prefix-length* received with route-distinguisher *route-distinguisher* on network instance *network-instance* and bgp instance *bgp-instance* is withdrawn because the route is received without a Gateway MAC Address and that is not allowed in an EVPN Interface-less bgp instance for VXLAN tunnels
Cause	This event is generated when a received IP Prefix route does not contain the required GW Mac and therefore it is not allowed in the local EVPN Interface-less bgp instance of the network-instance
Effect	The ip-prefix is not programmed in the route table of the network instance

15.11 evpnIpPrefixRouteWithdrawnDueToUnexpectedGwIp

Table 267: evpnIpPrefixRouteWithdrawnDueToUnexpectedGwIp properties

Property name	Value
Application name	evpn
Event name	evpnIpPrefixRouteWithdrawnDueToUnexpectedGwIp
Default severity	warning
Message format string	BGP-EVPN IP-PREFIX *ip-prefix* LENGTH *prefix-length* received with route-distinguisher *route-distinguisher* on network instance *network-instance* and bgp instance *bgp-instance* is withdrawn because the non-zero Gateway IP Address *gw-ip-address* received in the route is not allowed in an EVPN Interface-less bgp instance of the network-instance
Cause	This event is generated when a received Gateway IP Address in the IP Prefix routes is non-zero and therefore not allowed in the local EVPN Interface-less bgp instance of the network-instance

Property name	Value
Effect	The ip-prefix is not programmed in the route table of the network instance

15.12 evpnMacRouteAddDroppedDueToUnexpectedEthTag

Table 268: evpnMacRouteAddDroppedDueToUnexpectedEthTag properties

Property name	Value
Application name	evpn
Event name	evpnMacRouteAddDroppedDueToUnexpectedEthTag
Default severity	warning
Message format string	BGP-EVPN MAC *mac-address* IP *ip-address* received with route-distinguisher *route-distinguisher* add on network instance *network-instance* and bgp instance *bgp-instance* is dropped because the Ethernet Tag Identifier *received-ethernet-tag* received in the route, does not match locally configured Ethernet Tag Identifier *local-ethernet-tag* on the bgp-instance
Cause	This event is generated when a received Ethernet Tag Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The mac-address is not programmed in the bridge-table AND/OR the mac-address/ip-address pair is not programmed in the ARP or Neighbor discovery table

15.13 evpnMacRouteWithdrawDroppedDueToUnexpectedEthTag

Table 269: evpnMacRouteWithdrawDroppedDueToUnexpectedEthTag properties

Property name	Value
Application name	evpn
Event name	evpnMacRouteWithdrawDroppedDueToUnexpectedEthTag
Default severity	warning
Message format string	BGP-EVPN MAC *mac-address* IP *ip-address* received with route-distinguisher *route-distinguisher* delete on network instance *network-instance* and bgp instance *bgp-instance* is dropped because the Ethernet Tag Identifier *received-ethernet-tag* received in the route, does

Property name	Value
	not match locally configured Ethernet Tag Identifier *local-ethernet-tag* on the bgp-instance
Cause	This event is generated when a received Ethernet Tag Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The mac-address if programmed in the bridge-table AND/OR the mac-address/ip-address pair if programmed in the ARP or Neighbor discovery table, might not be removed

15.14 evpnMacRouteWithdrawnDueToUnexpectedVni

Table 270: evpnMacRouteWithdrawnDueToUnexpectedVni properties

Property name	Value
Application name	evpn
Event name	evpnMacRouteWithdrawnDueToUnexpectedVni
Default severity	warning
Message format string	BGP-EVPN MAC *mac-address* IP *ip-address* received with route-distinguisher *route-distinguisher* on network instance *network-instance* and bgp instance *bgp-instance* is withdrawn because the VXLAN Network Identifier *received-vni* received in the route, does not match locally configured VXLAN Network Identifier *local-vni* on the bgp-instance
Cause	This event is generated when a received VXLAN Network Identifier does not match the one configured locally on the bgp-instance in the network instance
Effect	The mac-address is not programmed in the bridge-table AND/OR the mac-address/ip-address pair is not programmed in the ARP or Neighbor discovery table

16 gnmi

16.1 globalConfigUpdate

Table 271: globalConfigUpdate properties

Property name	Value
Application name	gnmi
Event name	globalConfigUpdate
Default severity	informational
Message format string	gNMI server global configuration updated.
Cause	A global configuration change has been made, resulting in gNMI configuration being regenerated.
Effect	May result in gNMI server(s) start or stop depending on the configuration change.

16.2 gnmiServerStart

Table 272: gnmiServerStart properties

Property name	Value
Application name	gnmi
Event name	gnmiServerStart
Default severity	informational
Message format string	gNMI server started for network instance *network_instance* source address *source_address* port number *gnmi_socket*.
Cause	gNMI server has started for the mentioned network instance, source address and port number.
Effect	gNMI server is ready to receive and process requests for the mentioned network instance, source address and port number.

16.3 gnmiServerStop

Table 273: gnmiServerStop properties

Property name	Value
Application name	gnmi
Event name	gnmiServerStop
Default severity	informational
Message format string	gNMI server stopped for network *network_instance* source address *source_address* port number *gnmi_socket*.
Cause	gNMI server has stopped for the mentioned network instance, source address and port number.
Effect	gNMI server is not ready to receive and process requests for the mentioned network instance, source address and port number.

16.4 networkInstanceConfigUpdate

Table 274: networkInstanceConfigUpdate properties

Property name	Value
Application name	gnmi
Event name	networkInstanceConfigUpdate
Default severity	informational
Message format string	gNMI server network instance *network_instance* configuration updated.
Cause	A configuration change has been made in the mentioned network instance, resulting in gNMI server configuration being regenerated.
Effect	May result in gNMI server start or stop depending on the configuration change.

16.5 subscriptionEnd

Table 275: subscriptionEnd properties

Property name	Value
Application name	gnmi

Property name	Value
Event name	subscriptionEnd
Default severity	informational
Message format string	Subscription for path(s) *paths* requested by *peer_address*:*socket* has finished.
Cause	A subscription has finished based on the request from mentioned peer.
Effect	none.

16.6 subscriptionRequestReceived

Table 276: subscriptionRequestReceived properties

Property name	Value
Application name	gnmi
Event name	subscriptionRequestReceived
Default severity	informational
Message format string	Subscription request from peer *peer_address*:*socket* is received.
Cause	A subscription request is received from the mentioned peer.
Effect	gNMI server will process the request.

16.7 subscriptionStart

Table 277: subscriptionStart properties

Property name	Value
Application name	gnmi
Event name	subscriptionStart
Default severity	informational
Message format string	Subscription for path(s) *paths* requested by *peer_address*:*socket* has started.
Cause	A subscription has started based on the request from mentioned peer.
Effect	none.

16.8 unixSocketGnmiOperDown

Table 278: unixSocketGnmiOperDown properties

Property name	Value
Application name	gnmi
Event name	unixSocketGnmiOperDown
Default severity	critical
Message format string	Unix Domain Socket gNMI server is no longer operational.
Cause	The Unix domain socket gNMI server has transitioned from any other operational state to the down state.
Effect	Unix Domain Socket gNMI server is now down.

16.9 unixSocketGnmiOperUp

Table 279: unixSocketGnmiOperUp properties

Property name	Value
Application name	gnmi
Event name	unixSocketGnmiOperUp
Default severity	warning
Message format string	Unix domain socket gNMI server is operational.
Cause	The Unix domain socket gNMI server has transitioned from any other operational state to the up state.
Effect	Unix domain socket gNMI server is now up.

17 gnsi

17.1 gnsiAuthzPolicyFinalized

Table 280: gnsiAuthzPolicyFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiAuthzPolicyFinalized
Default severity	informational
Message format string	Authz gRPC authorization policy has been finalized on version *version* created on *created_on*
Cause	Authz has received a request to rotate the gRPC authorization policy, and a subsequent request to finalize it.
Effect	Requests to all gRPC servers on the system will authorize using the new policy. Reboots of the system will use the new policy rather than reverting to the previous.

17.2 gnsiAuthzPolicyInvalid

Table 281: gnsiAuthzPolicyInvalid properties

Property name	Value
Application name	gnsi
Event name	gnsiAuthzPolicyInvalid
Default severity	critical
Message format string	Authz gRPC authorization policy with version *version* created on *created_on* failed to validate - policy content invalid. Previous policy remains active.
Cause	Authz has received a request to rotate the gRPC authorization policy, with policy content that is invalid.
Effect	Requests to all gRPC servers on the system will authorize using the previous policy.

17.3 gnsiAuthzPolicyNotFinalized

Table 282: gnsiAuthzPolicyNotFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiAuthzPolicyNotFinalized
Default severity	critical
Message format string	Authz gRPC authorization policy with version *version* created on *created_on* was not finalized by client. Reverting to previous policy.
Cause	Authz has received a request to rotate the gRPC authorization policy, but did not received a subsequent finalization before the RPC was terminated.
Effect	Requests to all gRPC servers on the system will authorize using the previous policy.

17.4 gnsiAuthzPolicyRotate

Table 283: gnsiAuthzPolicyRotate properties

Property name	Value
Application name	gnsi
Event name	gnsiAuthzPolicyRotate
Default severity	informational
Message format string	Authz gRPC authorization policy has been rotated to version *version* created on *created_on*
Cause	gNSI server has received a request to rotate the gRPC authorization policy.
Effect	Requests to all gRPC servers on the system will authorize using the new policy. If a request is not recieved to finalize the rotation, the system will revert to the previous policy.

17.5 gnsiCertzRotate

Table 284: gnsiCertzRotate properties

Property name	Value
Application name	gnsi
Event name	gnsiCertzRotate
Default severity	informational
Message format string	Certz *artifact_type* has been rotated to version *version* created on *created_on*
Cause	Certz has received a request to rotate the specified certificate or bundle.
Effect	All gRPC servers without explicitly configured TLS server profiles will use the certificate and bundles provided. If a request is not received to finalize the rotation, the system will revert to the previous certificate and/or bundle/s.

17.6 gnsiCertzRotateFinalized

Table 285: gnsiCertzRotateFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiCertzRotateFinalized
Default severity	informational
Message format string	Certz *artifact_type* has been finalized on version *version* created on *created_on*
Cause	Certz has received a request to rotate the certificate and/or bundle/s, and a subsequent request to finalize it.
Effect	All gRPC servers without explicitly configured TLS server profiles will use the certificate and/or bundle/s provided. Reboots of the system will use the profile rather than reverting to the previous.

17.7 gnsiCertzRotateInvalid

Table 286: gnsiCertzRotateInvalid properties

Property name	Value
Application name	gnsi
Event name	gnsiCertzRotateInvalid
Default severity	critical
Message format string	Certz *artifact_type* with version *version* created on *created_on* failed to rotate. Previous *artifact_type* remains active. Error: *error*
Cause	Certz has received a request to rotate a certificate and/or bundle/s, but the RPC has failed with the provided error.
Effect	All gRPC servers without explicitly configured TLS server profiles will revert to using the previous certificate and/or bundle/s provided.

17.8 gnsiCertzRotateNotFinalized

Table 287: gnsiCertzRotateNotFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiCertzRotateNotFinalized
Default severity	critical
Message format string	Certz *artifact_type* with version *version* created on *created_on* was not finalized by client. Reverting to previous.
Cause	Certz has received a request to rotate the a certificate and/or bundle/s, but did not received a subsequent finalization before the RPC was terminated.
Effect	All gRPC servers without explicitly configured TLS server profiles will revert to using the previous certificate and/or bundle/s provided.

17.9 gnsiCredentialzRotateAccountCredentials

Table 288: gnsiCredentialzRotateAccountCredentials properties

Property name	**Value**
Application name	gnsi
Event name	gnsiCredentialzRotateAccountCredentials
Default severity	informational
Message format string	Credentialz *artifact_type* for user *username* has been rotated to version *version* created on *created_on*
Cause	Credentialz has received a request to rotate the specified aaa user credentials.
Effect	System will use the aaa user credentials provided. If a request is not received to finalize the rotation, the system will revert to the previous aaa user credentials.

17.10 gnsiCredentialzRotateAccountCredentialsFinalized

Table 289: gnsiCredentialzRotateAccountCredentialsFinalized properties

Property name	**Value**
Application name	gnsi
Event name	gnsiCredentialzRotateAccountCredentialsFinalized
Default severity	informational
Message format string	Credentialz *artifact_type* for user *username* has been finalized on version *version* created on *created_on*
Cause	Credentialz has received a request to rotate aaa user credentials, and a subsequent request to finalize it.
Effect	System will use the aaa user credentials provided. Reboots of the system will use the aaa user credentials rather than reverting to the previous.

17.11 gnsiCredentialzRotateAccountCredentialsInvalid

Table 290: gnsiCredentialzRotateAccountCredentialsInvalid properties

Property name	Value
Application name	gnsi
Event name	gnsiCredentialzRotateAccountCredentialsInvalid
Default severity	critical
Message format string	Credentialz *artifact_type* for user *username* with version *version* created on *created_on* failed to rotate. Previous *artifact_type* remains active. Error: *error*
Cause	Credentialz has received a request to rotate aaa user credentials, but the RPC has failed with the provided error.
Effect	System will revert to using the previous aaa user credentials provided.

17.12 gnsiCredentialzRotateAccountCredentialsNotFinalized

Table 291: gnsiCredentialzRotateAccountCredentialsNotFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiCredentialzRotateAccountCredentialsNotFinalized
Default severity	critical
Message format string	Credentialz *artifact_type* for user *username* with version *version* created on *created_on* was not finalized by client. Reverting to previous.
Cause	Credentialz has received a request to rotate aaa user credentials, but did not received a subsequent finalization before the RPC was terminated.
Effect	System will revert to using the previous aaa user credentials provided.

17.13 gnsiCredentialzRotateHostParameters

Table 292: gnsiCredentialzRotateHostParameters properties

Property name	Value
Application name	gnsi
Event name	gnsiCredentialzRotateHostParameters
Default severity	informational
Message format string	Credentialz *artifact_type* has been rotated to version *version* created on *created_on*
Cause	Credentialz has received a request to rotate the specified ssh host parameters.
Effect	All ssh servers will use the ssh host parameters provided. If a request is not received to finalize the rotation, the system will revert to the previous ssh host parameters.

17.14 gnsiCredentialzRotateHostParametersFinalized

Table 293: gnsiCredentialzRotateHostParametersFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiCredentialzRotateHostParametersFinalized
Default severity	informational
Message format string	Credentialz *artifact_type* has been finalized on version *version* created on *created_on*
Cause	Credentialz has received a request to rotate ssh host parameters, and a subsequent request to finalize it.
Effect	All ssh servers will use the ssh host parameters provided. Reboots of the system will use the ssh host parameters rather than reverting to the previous.

17.15 gnsiCredentialzRotateHostParametersInvalid

Table 294: gnsiCredentialzRotateHostParametersInvalid properties

Property name	Value
Application name	gnsi
Event name	gnsiCredentialzRotateHostParametersInvalid
Default severity	critical
Message format string	Credentialz *artifact_type* with version *version* created on *created_on* failed to rotate. Previous *artifact_type* remains active. Error: *error*
Cause	Credentialz has received a request to rotate ssh host parameters, but the RPC has failed with the provided error.
Effect	All ssh servers will revert to using the previous ssh host parameters provided.

17.16 gnsiCredentialzRotateHostParametersNotFinalized

Table 295: gnsiCredentialzRotateHostParametersNotFinalized properties

Property name	Value
Application name	gnsi
Event name	gnsiCredentialzRotateHostParametersNotFinalized
Default severity	critical
Message format string	Credentialz *artifact_type* with version *version* created on *created_on* was not finalized by client. Reverting to previous.
Cause	Credentialz has received a request to rotate ssh host parameters, but did not received a subsequent finalization before the RPC was terminated.
Effect	All ssh servers will revert to using the previous ssh host parameters provided.

18 gribi

18.1 globalConfigUpdate

Table 296: globalConfigUpdate properties

Property name	Value
Application name	gribi
Event name	globalConfigUpdate
Default severity	informational
Message format string	Gribi server global configuration updated.
Cause	A global configuration change has been made, resulting in Gribi configuration being regenerated.
Effect	May result in Gribi server(s) start or stop depending on the configuration change.

18.2 gribiServerStart

Table 297: gribiServerStart properties

Property name	Value
Application name	gribi
Event name	gribiServerStart
Default severity	informational
Message format string	Gribi server started for network instance *network_instance* source address *source_address* port number *gribi_socket*.
Cause	Gribi server has started for the mentioned network instance, source address and port number.
Effect	Gribi server is ready to receive and process requests for the mentioned network instance, source address and port number.

18.3 gribiServerStop

Table 298: gribiServerStop properties

Property name	Value
Application name	gribi
Event name	gribiServerStop
Default severity	informational
Message format string	Gribi server stopped for network *network_instance* source address *source_address* port number *gribi_socket*.
Cause	Gribi server has stopped for the mentioned network instance, source address and port number.
Effect	Gribi server is not ready to receive and process requests for the mentioned network instance, source address and port number.

18.4 networkInstanceConfigUpdate

Table 299: networkInstanceConfigUpdate properties

Property name	Value
Application name	gribi
Event name	networkInstanceConfigUpdate
Default severity	informational
Message format string	Gribi server network instance *network_instance* configuration updated.
Cause	A configuration change has been made in the mentioned network instance, resulting in Gribi server configuration being regenerated.
Effect	May result in Gribi server start or stop depending on the configuration change.

18.5 unixSocketGribiOperDown

Table 300: unixSocketGribiOperDown properties

Property name	Value
Application name	gribi

Property name	Value
Event name	unixSocketGribiOperDown
Default severity	critical
Message format string	Unix Domain Socket Gribi server is no longer operational.
Cause	The Unix domain socket Gribi server has transitioned from any other operational state to the down state.
Effect	Unix Domain Socket Gribi server is now down.

18.6 unixSocketGribiOperUp

Table 301: unixSocketGribiOperUp properties

Property name	Value
Application name	gribi
Event name	unixSocketGribiOperUp
Default severity	warning
Message format string	Unix domain socket Gribi server is operational.
Cause	The Unix domain socket Gribi server has transitioned from any other operational state to the up state.
Effect	Unix domain socket Gribi server is now up.

19 grpc

19.1 configUpdate

Table 302: configUpdate properties

Property name	Value
Application name	grpc
Event name	configUpdate
Default severity	informational
Message format string	gRPC server *name* configuration updated.
Cause	A configuration change has been made in the mentioned grpc server, resulting in gRPC server configuration being regenerated.
Effect	May result in gRPC server start or stop depending on the configuration change.

19.2 grpcServerStart

Table 303: grpcServerStart properties

Property name	Value
Application name	grpc
Event name	grpcServerStart
Default severity	informational
Message format string	gRPC server *name* started for network instance *network_instance* source address *source_address* port number *grpc_socket*.
Cause	gRPC server has started for the mentioned network instance, source address and port number.
Effect	gRPC server is ready to receive and process requests for the mentioned network instance, source address and port number.

19.3 grpcServerStop

Table 304: grpcServerStop properties

Property name	Value
Application name	grpc
Event name	grpcServerStop
Default severity	informational
Message format string	gRPC server *name* stopped for network *network_instance* source address *source_address* port number *grpc_socket*.
Cause	gRPC server has stopped for the mentioned network instance, source address and port number.
Effect	gRPC server is not ready to receive and process requests for the mentioned network instance, source address and port number.

19.4 subscriptionEnd

Table 305: subscriptionEnd properties

Property name	Value
Application name	grpc
Event name	subscriptionEnd
Default severity	informational
Message format string	Subscription for path(s) *paths* requested by *peer_address*:*socket* has finished.
Cause	A subscription has finished based on the request from mentioned peer.
Effect	none.

19.5 subscriptionRequestReceived

Table 306: subscriptionRequestReceived properties

Property name	Value
Application name	grpc
Event name	subscriptionRequestReceived

Property name	Value
Default severity	informational
Message format string	Subscription request from peer *peer_address*:*socket* is received.
Cause	A subscription request is received from the mentioned peer.
Effect	gRPC server will process the request.

19.6 subscriptionStart

Table 307: subscriptionStart properties

Property name	Value
Application name	grpc
Event name	subscriptionStart
Default severity	informational
Message format string	Subscription for path(s) *paths* requested by *peer_address*:*socket* has started.
Cause	A subscription has started based on the request from mentioned peer.
Effect	none.

19.7 unixSocketGrpcOperDown

Table 308: unixSocketGrpcOperDown properties

Property name	Value
Application name	grpc
Event name	unixSocketGrpcOperDown
Default severity	critical
Message format string	Unix domain socket of gRPC server *name* is no longer operational.
Cause	The Unix domain socket of gRPC server has transitioned from any other operational state to the down state.
Effect	Unix domain socket of gRPC server is now down.

19.8 unixSocketGrpcOperUp

Table 309: unixSocketGrpcOperUp properties

Property name	Value
Application name	grpc
Event name	unixSocketGrpcOperUp
Default severity	warning
Message format string	Unix domain socket of gRPC server *name* is operational.
Cause	The Unix domain socket of gRPC server has transitioned from any other operational state to the up state.
Effect	Unix domain socket of gRPC server is now up.

20 igmp

20.1 igmpCModeRxQueryVersionMismatch

Table 310: igmpCModeRxQueryVersionMismatch properties

Property name	Value
Application name	igmp
Event name	igmpCModeRxQueryVersionMismatch
Default severity	warning
Message format string	Network-instance *network_instance* - Mismatch between the interface *subinterface* compatible mode(*igmpInterfaceOperVersion*) and the version of the IGMP query (version *igmpQuerierVersion*) received on the interface.
Cause	This event is generated when the IGMP interface receives a query with a version that is higher than the interface's compatible mode.
Effect	IGMP interfaces will ignore any Queries with a version higher than the interface's compatibility mode.

20.2 igmpMaxNumberOfGroupSourcesReached

Table 311: igmpMaxNumberOfGroupSourcesReached properties

Property name	Value
Application name	igmp
Event name	igmpMaxNumberOfGroupSourcesReached
Default severity	warning
Message format string	Network-instance *network_instance* - The number of group/source combinations learned on interface *subinterface* has exceeded the maximum limit of *igmpInterfaceMaxGroupSources*.
Cause	This event is generated when an attempt is made to learn a source when the number of group/source combinations on the IGMP interface is equal to the maximum number of group-sources configured on the interface.

Property name	Value
Effect	IGMP interfaces will not learn any new sources for a given group when the configured maximum number of group-sources has been reached.

20.3 igmpMaxNumberOfGroupsReached

Table 312: igmpMaxNumberOfGroupsReached properties

Property name	Value
Application name	igmp
Event name	igmpMaxNumberOfGroupsReached
Default severity	warning
Message format string	Network-instance *network_instance* - The number of groups learned on interface *subinterface* has exceeded the maximum limit of *igmp InterfaceMaxGroups*.
Cause	This event is generated when an attempt is made to learn a group when the number of groups on the IGMP interface is equal to the maximum number of groups configured on the interface.
Effect	IGMP interfaces will not learn any new groups when the configured maximum number of groups has been reached.

20.4 igmpMaxNumberOfSourcesReached

Table 313: igmpMaxNumberOfSourcesReached properties

Property name	Value
Application name	igmp
Event name	igmpMaxNumberOfSourcesReached
Default severity	warning
Message format string	Network-instance *network_instance* - The number of sources learned on interface *subinterface* has exceeded the maximum limit of *igmp InterfaceMaxSources*.
Cause	This event is generated when an attempt is made to learn a source when the number of sources for this group on the IGMP interface is equal to the maximum number of sources per group configured on the interface.

Property name	Value
Effect	IGMP interfaces will not learn any new sources for a given group when the configured maximum number of sources for the group has been reached.

20.5 igmpRxQueryVersionMismatch

Table 314: igmpRxQueryVersionMismatch properties

Property name	Value
Application name	igmp
Event name	igmpRxQueryVersionMismatch
Default severity	warning
Message format string	Network-instance *network_instance* - IGMPv*igmpQuerierVersion* query received on interface *subinterface* configured as IGMPv*igmpInterface AdminVersion*.
Cause	This event is generated when the IGMP interface is configured as IGMPv3 and receives an IGMPv1 Query or IGMPv2 General Query.
Effect	IGMP interfaces configured as IGMPv3 will ignore IGMPv1 and IGMPv2 General Queries.

21 isis

21.1 isisAdjacencyBfdSessionSetupFailed

Table 315: isisAdjacencyBfdSessionSetupFailed properties

Property name	Value
Application name	isis
Event name	isisAdjacencyBfdSessionSetupFailed
Default severity	warning
Message format string	In network-instance *network_instance*, BFD session setup failed for the *level* IS-IS adjacency with system *sys_id*, using interface *subinterface*. Failure reason: *bfd_failure_reason*.
Cause	This event is generated when BFD session setup fails with an adjacent neighbor.
Effect	Fast failure detection may not be possible.

21.2 isisAdjacencyChange

Table 316: isisAdjacencyChange properties

Property name	Value
Application name	isis
Event name	isisAdjacencyChange
Default severity	warning
Message format string	In network-instance *network_instance*, the *level* IS-IS adjacency with system *sys_id*, using interface *subinterface*, moved to state *adj_state*.
Cause	This event is generated when an IS-IS adjacency enters or leaves the up state.
Effect	IS-IS traffic can only be forwarded along adjacencies that are up.

21.3 isisAdjacencyRestartStatusChange

Table 317: isisAdjacencyRestartStatusChange properties

Property name	Value
Application name	isis
Event name	isisAdjacencyRestartStatusChange
Default severity	warning
Message format string	In network-instance *network_instance*, the graceful restart status for the *level* IS-IS adjacency on interface *subinterface* moved to new state *restart_status*.
Cause	This event is generated when the graceful restart status of a neighbor changes.
Effect	None

21.4 isisAreaMismatch

Table 318: isisAreaMismatch properties

Property name	Value
Application name	isis
Event name	isisAreaMismatch
Default severity	warning
Message format string	In network-instance *network_instance*, a level1 PDU was received on interface *subinterface* with no Area Addresses matching the areas to which this IS router belongs. The PDU starts with: *pdu_fragment*
Cause	This event is generated to alert of a possible area-id misconfiguration inside a L1 area.
Effect	L1 adjacency cannot form

21.5 isisAuthDataFail

Table 319: isisAuthDataFail properties

Property name	Value
Application name	isis
Event name	isisAuthDataFail
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* PDU was received on interface *subinterface* with unexpected or incorrect data in the Authentication TLV. The PDU starts with: *pdu_fragment*
Cause	This event could be caused by incorrect keychain configuration in this router or its neighbor.
Effect	PDUs are dropped, with the effect depending on the PDU type

21.6 isisAuthTypeMismatch

Table 320: isisAuthTypeMismatch properties

Property name	Value
Application name	isis
Event name	isisAuthTypeMismatch
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* PDU was received on interface *subinterface* with an unrecognized or unsupported authentication type in TLV 10. The PDU starts with: *pdu_fragment*
Cause	This event could be caused by incorrect keychain configuration in this router or its neighbor.
Effect	PDUs are dropped, with the effect depending on the PDU type

21.7 isisCircuitIdsExhausted

Table 321: isisCircuitIdsExhausted properties

Property name	Value
Application name	isis
Event name	isisCircuitIdsExhausted
Default severity	warning
Message format string	In network-instance *network_instance*, the IS-IS interface *subinterface* is operationally down because the limit of 255 circuit IDs available to LAN interfaces was reached.
Cause	This event is caused by having too many LAN interfaces.
Effect	LAN adjacencies are not formed

21.8 isisCircuitMtuTooLow

Table 322: isisCircuitMtuTooLow properties

Property name	Value
Application name	isis
Event name	isisCircuitMtuTooLow
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* LSP PDU or SNP PDU could not be transmitted on interface *subinterface* because the IP MTU is only *operational_subif_mtu* and an MTU of at least *required_mtu* is required.
Cause	The port MTU is too small and/or the lsp-mtu-size is too large.
Effect	PDUs are dropped

21.9 isisCorruptedLspDetected

Table 323: isisCorruptedLspDetected properties

Property name	Value
Application name	isis

Property name	Value
Event name	isisCorruptedLspDetected
Default severity	warning
Message format string	In network-instance *network_instance*, the LSP PDU with ID *lsp_id* in the *level* database has become corrupted.
Cause	Memory corruption or other.
Effect	LSP is removed

21.10 isisLdpSyncExited

Table 324: isisLdpSyncExited properties

Property name	Value
Application name	isis
Event name	isisLdpSyncExited
Default severity	warning
Message format string	In network-instance *network_instance*, the LDP synchronization state has ended on IS-IS interface *subinterface*, and now the state is *sync_state*
Cause	The LDP synchronization timer can be stopped because of a tools command, hold-down timer expiry or indication from the LDP peer that End-of-LIB has been received. When LDP sync is exited IS-IS resumes advertising a normal metric for the interface.
Effect	Transit traffic can start using this interface again.

21.11 isisLdpSyncTimerStarted

Table 325: isisLdpSyncTimerStarted properties

Property name	Value
Application name	isis
Event name	isisLdpSyncTimerStarted
Default severity	warning

Property name	Value
Message format string	In network-instance *network_instance*, the LDP synchronization timer has started on IS-IS interface *subinterface*
Cause	The sync timer is started when LDP synchronization is configured and the LDP adjacency comes up with the LDP peer. When this timer expires IS-IS will resume advertisement of a normal metric for the interface.
Effect	Transit traffic will continue to avoid using this interface.

21.12 isisLspFragmentTooLarge

Table 326: isisLspFragmentTooLarge properties

Property name	Value
Application name	isis
Event name	isisLspFragmentTooLarge
Default severity	warning
Message format string	In network-instance *network_instance*, the *level* LSP PDU fragment *lsp_id* received on interface *subinterface* could not be accepted because the configured LSP MTU size is too small. An LSP MTU size of at least *required_lsp_mtu* bytes is required.
Cause	Misconfiguration of LSP MTU size
Effect	LSP PDU is not accepted

21.13 isisLspPurge

Table 327: isisLspPurge properties

Property name	Value
Application name	isis
Event name	isisLspPurge
Default severity	warning
Message format string	In network-instance *network_instance*, the LSP PDU with ID *lsp_id* in the *level* database has been purged by *purge_originator*.
Cause	LSP lifetime expired or other reason

Property name	Value
Effect	The PDU is removed

21.14 isisLspSequenceNumberSkip

Table 328: isisLspSequenceNumberSkip properties

Property name	Value
Application name	isis
Event name	isisLspSequenceNumberSkip
Default severity	warning
Message format string	In network-instance *network_instance*, the LSP with id *lsp_id* in the *level* database was re-originated with a sequence number that incremented by more than one.
Cause	There may be another IS router configured with the same system ID.
Effect	None

21.15 isisMaxAreaAddressesMismatch

Table 329: isisMaxAreaAddressesMismatch properties

Property name	Value
Application name	isis
Event name	isisMaxAreaAddressesMismatch
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* PDU was received on interface *subinterface* with an unexpected Max Area Addresses value in the IS-IS PDU header. The PDU starts with: *pdu_fragment*
Cause	Misconfiguration of max area addresses in the neighbor
Effect	The PDU is dropped

21.16 isisMaxLspSequenceNumberExceeded

Table 330: isisMaxLspSequenceNumberExceeded properties

Property name	Value
Application name	isis
Event name	isisMaxLspSequenceNumberExceeded
Default severity	warning
Message format string	In network-instance *network_instance*, the LSP with id *lsp_id* in the *level* database was purged because the sequence number was already at its maximum value and could not be incremented.
Cause	A possible cause could be that the same system-id is configured on multiple systems; when 2 systems have the same system-id they both keep incrementing the LSP sequence number, causing the sequence counter to rollover.
Effect	The PDU is purged and reachability may be temporarily lost

21.17 isisOverloadEntry

Table 331: isisOverloadEntry properties

Property name	Value
Application name	isis
Event name	isisOverloadEntry
Default severity	warning
Message format string	In the IS-IS instance of network-instance *network_instance*, the *level* database has entered the overload state.
Cause	Overload bit configuration
Effect	No transit traffic is routed through the overloaded router.

21.18 isisOverloadExit

Table 332: isisOverloadExit properties

Property name	Value
Application name	isis
Event name	isisOverloadExit
Default severity	warning
Message format string	In the IS-IS instance of network-instance *network_instance*, the *level* database has exited from the overload state.
Cause	Overload bit configuration
Effect	Transit traffic can again be routed through the router.

21.19 isisOwnLspPurge

Table 333: isisOwnLspPurge properties

Property name	Value
Application name	isis
Event name	isisOwnLspPurge
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* LSP PDU was received with the system ID of this IS router and age equal to zero. The purge originator was *purge_originator*.
Cause	LSP lifetime expired or other reason
Effect	The PDU is removed

21.20 isisSystemIdLengthMismatch

Table 334: isisSystemIdLengthMismatch properties

Property name	Value
Application name	isis
Event name	isisSystemIdLengthMismatch

Property name	Value
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* PDU was received on interface *subinterface* with an unexpected System ID length in the IS-IS PDU header. The PDU starts with: *pdu_fragment*
Cause	Misconfiguration of system ID length in the neighbor
Effect	The PDU is dropped

21.21 isisVersionMismatch

Table 335: isisVersionMismatch properties

Property name	Value
Application name	isis
Event name	isisVersionMismatch
Default severity	warning
Message format string	In network-instance *network_instance*, a *level* PDU was received on interface *subinterface* with an IS-IS protocol version not matching the expected value. The PDU starts with: *pdu_fragment*
Cause	Unsupported IS-IS version
Effect	PDUs cannot be exchanged

22 json

22.1 authenticationError

Table 336: authenticationError properties

Property name	Value
Application name	json
Event name	authenticationError
Default severity	informational
Message format string	No username/password received, authentication needed
Cause	A user has failed to authenticate.
Effect	That user can't establish a configuration session.

22.2 globalConfigUpdate

Table 337: globalConfigUpdate properties

Property name	Value
Application name	json
Event name	globalConfigUpdate
Default severity	informational
Message format string	JSON RPC server global configuration updated.
Cause	A global configuration change has been made, resulting in json rpc configuration being regenerated.
Effect	May result in json rpc process(es) start or stop depending on the configuration change.

22.3 httpJsonRpcOperDown

Table 338: httpJsonRpcOperDown properties

Property name	Value
Application name	json
Event name	httpJsonRpcOperDown
Default severity	critical
Message format string	HTTP JSON RPC server for network instance *network_instance* is no longer operational.
Cause	The httpJsonRpcOperDown event is generated when HTTP JSON RPC server on the mentioned network instance has transitioned from any other operational state to the down state.
Effect	HTTP JSON RPC server on the mentioned network instance is now down.

22.4 httpJsonRpcOperUp

Table 339: httpJsonRpcOperUp properties

Property name	Value
Application name	json
Event name	httpJsonRpcOperUp
Default severity	warning
Message format string	HTTP JSON RPC server for network instance *network_instance* is operational.
Cause	The httpJsonRpcOperUp event is generated when HTTP JSON RPC server on the mentioned network instance has transitioned from any other operational state to the up state.
Effect	HTTP JSON RPC server on the mentioned network instance is now up.

22.5 httpsJsonRpcOperDown

Table 340: httpsJsonRpcOperDown properties

Property name	Value
Application name	json
Event name	httpsJsonRpcOperDown
Default severity	critical
Message format string	HTTPS JSON RPC server for network instance *network_instance* is no longer operational.
Cause	The httpsJsonRpcOperDown event is generated when HTTPs JSON RPC server on the mentioned network instance has transitioned from any other operational state to the down state.
Effect	HTTPS JSON RPC server on the mentioned network instance is now down.

22.6 httpsJsonRpcOperUp

Table 341: httpsJsonRpcOperUp properties

Property name	Value
Application name	json
Event name	httpsJsonRpcOperUp
Default severity	warning
Message format string	HTTPS JSON RPC server for network instance *network_instance* is operational.
Cause	The httpsJsonRpcOperUp event is generated when HTTPs JSON RPC server on the mentioned network instance has transitioned from any other operational state to the up state.
Effect	HTTPS JSON RPC server on the mentioned network instance is now up.

22.7 jsonRpcRequestReceived

Table 342: jsonRpcRequestReceived properties

Property name	Value
Application name	json
Event name	jsonRpcRequestReceived
Default severity	informational
Message format string	Request received for session id *session_id* username *username*.
Cause	A JSON RPC Request is received.
Effect	JSON RPC server processes That Requset.

22.8 jsonRpcResponseSent

Table 343: jsonRpcResponseSent properties

Property name	Value
Application name	json
Event name	jsonRpcResponseSent
Default severity	informational
Message format string	Response sent for session id *session_id* username *username*.
Cause	A JSON RPC Response is sent.
Effect	none.

22.9 networkInstanceConfigUpdate

Table 344: networkInstanceConfigUpdate properties

Property name	Value
Application name	json
Event name	networkInstanceConfigUpdate
Default severity	informational

Property name	Value
Message format string	JSON RPC server network instance *network_instance* configuration updated.
Cause	A configuration change has been made in the mentioned network instance, resulting in json rpc configuration being regenerated.
Effect	May result in json rpc process(es) start or stop depending on the configuration change.

22.10 unixSocketJsonRpcOperDown

Table 345: unixSocketJsonRpcOperDown properties

Property name	Value
Application name	json
Event name	unixSocketJsonRpcOperDown
Default severity	critical
Message format string	Unix Domain Socket JSON RPC server is no longer operational.
Cause	The Unix Domain Socket JSON RPC server has transitioned from any other operational state to the down state.
Effect	Unix Domain Socket JSON RPC server is now down.

22.11 unixSocketJsonRpcOperUp

Table 346: unixSocketJsonRpcOperUp properties

Property name	Value
Application name	json
Event name	unixSocketJsonRpcOperUp
Default severity	warning
Message format string	Unix Domain Socket JSON RPC server is operational.
Cause	The Unix Domain Socket JSON RPC server has transitioned from any other operational state to the up state.
Effect	Unix Domain Socket JSON RPC server is now up.

22.12 userAuthenticated

Table 347: userAuthenticated properties

Property name	Value
Application name	json
Event name	userAuthenticated
Default severity	informational
Message format string	User *username* authenticated.
Cause	A user has been successfully authenticated.
Effect	That user is ready to start a configuration session.

22.13 userAuthenticationErrorWrongPassword

Table 348: userAuthenticationErrorWrongPassword properties

Property name	Value
Application name	json
Event name	userAuthenticationErrorWrongPassword
Default severity	informational
Message format string	User *username* authentication failure, invalid username or password.
Cause	A user has failed to authenticate.
Effect	That user can't establish a configuration session.

23 lag

23.1 lagDown

Table 349: lagDown properties

Property name	Value
Application name	lag
Event name	lagDown
Default severity	warning
Message format string	LAG Interface *interface_name*: The operational state has transitioned to Down
Cause	This warning is generated when a LAG transitions to the down state.
Effect	The LAG is now down and any associated subinterfaces will also be brought down.

23.2 lagDownMinLinks

Table 350: lagDownMinLinks properties

Property name	Value
Application name	lag
Event name	lagDownMinLinks
Default severity	warning
Message format string	LAG Interface *interface_name*: The active number of member links has fallen below the min-links threshold
Cause	This warning is generated when a LAG transitions to the down state because the number of active links has dropped below the min-link threshold
Effect	The LAG is now down and any associated subinterfaces will also be brought down.

23.3 lagMemberLinkAdded

Table 351: lagMemberLinkAdded properties

Property name	Value
Application name	lag
Event name	lagMemberLinkAdded
Default severity	notice
Message format string	LAG Interface *interface_name*: The member-link *member-interface* has been added
Cause	This notification is generated when a new member-link is added to a LAG.
Effect	A new member link is now available to the LAG bundle.

23.4 lagMemberLinkRemoved

Table 352: lagMemberLinkRemoved properties

Property name	Value
Application name	lag
Event name	lagMemberLinkRemoved
Default severity	notice
Message format string	LAG Interface *interface_name*: The member-link *member-interface* has been removed
Cause	This notification is generated when a new member-link is removed from a LAG.
Effect	The specified interfaces is no longer a member of the LAG bundle.

23.5 lagMemberOperDown

Table 353: lagMemberOperDown properties

Property name	Value
Application name	lag
Event name	lagMemberOperDown

Property name	Value
Default severity	warning
Message format string	LAG Interface *interface_name*: The member-link *member-interface* operational state has transitioned to Down
Cause	This notification is generated when a member-link transitions to the down state.
Effect	The member link is now down and will not forward traffic.

23.6 lagMemberOperUp

Table 354: lagMemberOperUp properties

Property name	Value
Application name	lag
Event name	lagMemberOperUp
Default severity	warning
Message format string	LAG Interface *interface_name*: The member-link *member-interface* operational state has transitioned to Up
Cause	This notification is generated when a member-link transitions to the up state.
Effect	The member link is now operational.

23.7 lagUp

Table 355: lagUp properties

Property name	Value
Application name	lag
Event name	lagUp
Default severity	notice
Message format string	LAG Interface *interface_name*: The operational state has transitioned to Up
Cause	This notification is generated when a LAG transitions to the up state.

Property name	Value
Effect	The LAG is now operational.

24 license

24.1 licenseExpirySoon

Table 356: licenseExpirySoon properties

Property name	Value
Application name	license
Event name	licenseExpirySoon
Default severity	warning
Message format string	License *license_name* expires at *expires_at_date_time*, current time: *current_date_time*
Cause	The license specified will expire in less than 30 days.
Effect	If no new license is provided before the expiry, the system becomes unlicensed.

25 linux

25.1 cpuUsageCritical

Table 357: cpuUsageCritical properties

Property name	Value
Application name	linux
Event name	cpuUsageCritical
Default severity	critical
Message format string	CPU utilization on *component_type* module *slot* is above 90% on average for the last minute, current usage *cpu_usage_percentage*%
Cause	Applications or other system tasks have consumed more than 90% of available CPU resources on average over the last minute.
Effect	Processes may be scheduled at a slower rate than required, resulting in potential application failures or slow downs.

25.2 cpuUsageHigh

Table 358: cpuUsageHigh properties

Property name	Value
Application name	linux
Event name	cpuUsageHigh
Default severity	warning
Message format string	CPU utilization on *component_type* module *slot* is above 80% on average for the last minute, current usage *cpu_usage_percentage*%
Cause	Applications or other system tasks have consumed more than 80% of available CPU resources on average over the last minute.
Effect	No immediate effect, if utilization continues to increase, processes may be scheduled at a slower rate than required, resulting in potential application failures or slow downs.

25.3 cpuUsageNormal

Table 359: cpuUsageNormal properties

Property name	Value
Application name	linux
Event name	cpuUsageNormal
Default severity	notice
Message format string	CPU utilization on *component_type* module *slot* is below 70% on average for the last minute, current usage *cpu_usage_percentage*%
Cause	CPU consumption on the specified slot has returned to normal levels - below 70%, after triggering a cpuUsageHigh/cpuUsageCritical event.
Effect	None.

25.4 dateAndTimeChanged

Table 360: dateAndTimeChanged properties

Property name	Value
Application name	linux
Event name	dateAndTimeChanged
Default severity	notice
Message format string	System date and time changed to *date_and_time*
Cause	The system time has been changed either manually, or via NTP, to the specified time.
Effect	Local time on the system has changed.

25.5 domainChanged

Table 361: domainChanged properties

Property name	Value
Application name	linux

Property name	Value
Event name	domainChanged
Default severity	informational
Message format string	System domain name changed to *domain_name*
Cause	System configuration change to the domain name has been made.
Effect	The system uses the new domain name.

25.6 hostnameChanged

Table 362: hostnameChanged properties

Property name	Value
Application name	linux
Event name	hostnameChanged
Default severity	informational
Message format string	System host name changed to *host_name*
Cause	System configuration change to the host name has been made.
Effect	The system uses the new host name.

25.7 memoryUsageCritical

Table 363: memoryUsageCritical properties

Property name	Value
Application name	linux
Event name	memoryUsageCritical
Default severity	critical
Message format string	Memory utilization on *component_type* module *slot* is above 90%, current usage *memory_usage_percentage*%
Cause	Applications or other in-memory items have consumed more than 90% of the memory on the specified module.

Property name	Value
Effect	No immediate effect, if utilization continues to increase, new memory allocations may fail, resulting in potential application failures.

25.8 memoryUsageFull

Table 364: memoryUsageFull properties

Property name	Value
Application name	linux
Event name	memoryUsageFull
Default severity	emergency
Message format string	Memory utilization on *component_type* module *slot* is full
Cause	Applications or other in-memory items have consumed 100% of the memory on the specified module.
Effect	Further memory allocations will fail, likely leading to application failures and eventual module restart.

25.9 memoryUsageHigh

Table 365: memoryUsageHigh properties

Property name	Value
Application name	linux
Event name	memoryUsageHigh
Default severity	warning
Message format string	Memory utilization on *component_type* module *slot* is above 70%, current usage *memory_usage_percentage*%
Cause	Applications or other in-memory items have consumed more than 70% of the memory on the specified slot.
Effect	No immediate effect, if utilization continues to increase, new memory allocations may fail, resulting in potential application failures.

25.10 memoryUsageNormal

Table 366: memoryUsageNormal properties

Property name	Value
Application name	linux
Event name	memoryUsageNormal
Default severity	notice
Message format string	Memory utilization on *component_type* module *slot* is below 60%, current usage *memory_usage_percentage*%
Cause	Memory consumption on the specified slot has returned to normal levels - below 60%
Effect	None.

25.11 partitionStateChange

Table 367: partitionStateChange properties

Property name	Value
Application name	linux
Event name	partitionStateChange
Default severity	alert
Message format string	Partition *partition* has changed state to *current_state*
Cause	The specified partition has transitioned to a new state.
Effect	Depending on the state, the partition may now be unusable, read-only, or read-write.

25.12 partitionUsageCritical

Table 368: partitionUsageCritical properties

Property name	Value
Application name	linux
Event name	partitionUsageCritical

Property name	Value
Default severity	critical
Message format string	Partition *partition_label* usage on *component_type* module *slot* is higher than 90%, current usage *partition_usage_percentage*%
Cause	The specified partition is almost full, and action should be taken to remove unneeded files.
Effect	None.

25.13 partitionUsageFull

Table 369: partitionUsageFull properties

Property name	Value
Application name	linux
Event name	partitionUsageFull
Default severity	alert
Message format string	Partition *partition_label* on *component_type* module *slot* is full
Cause	The specified partition is full.
Effect	Write actions to this partition will fail.

25.14 partitionUsageNormal

Table 370: partitionUsageNormal properties

Property name	Value
Application name	linux
Event name	partitionUsageNormal
Default severity	notice
Message format string	Partition *partition_label* on *component_type* module *slot* is below 70%, current usage *partition_usage_percentage*%
Cause	Utilization of the specified partition is below 70%, after previously being higher than 80%.
Effect	None.

25.15 partitionUsageWarning

Table 371: partitionUsageWarning properties

Property name	Value
Application name	linux
Event name	partitionUsageWarning
Default severity	warning
Message format string	Partition *partition_label* usage on *component_type* module *slot* is higher than 80%, current usage *partition_usage_percentage*%
Cause	The specified partition is almost full, and action should be taken to remove unneeded files.
Effect	None.

25.16 serviceConfigChanged

Table 372: serviceConfigChanged properties

Property name	Value
Application name	linux
Event name	serviceConfigChanged
Default severity	notice
Message format string	Service *service_name* configuration changed, service reloaded
Cause	The specified service configuration has been changed, and linux_mgr has reloaded the service.
Effect	New configuration for the service is now in effect.

25.17 serviceDownInNetworkInstance

Table 373: serviceDownInNetworkInstance properties

Property name	Value
Application name	linux

Property name	Value
Event name	serviceDownInNetworkInstance
Default severity	warning
Message format string	Service *service_name* is no longer operational in network instance *net_inst*
Cause	The specified service has been disabled in the specified network instance.
Effect	Functionality provided by the service is no longer available in the specified network instance.

25.18 serviceUpInNetworkInstance

Table 374: serviceUpInNetworkInstance properties

Property name	Value
Application name	linux
Event name	serviceUpInNetworkInstance
Default severity	notice
Message format string	Service *service_name* is now operational in network instance *net_inst*
Cause	The specified service has been started in the specified network instance.
Effect	Functionality provided by the service is now available in the specified network instance.

25.19 tlsProfileExpired

Table 375: tlsProfileExpired properties

Property name	Value
Application name	linux
Event name	tlsProfileExpired
Default severity	warning
Message format string	Certificate in TLS profile *tls_profile* has expired

Property name	Value
Cause	The certificate used in the specified TLS profile has an expiration date in the past.
Effect	Authentication using the specified TLS profile may fail.

25.20 tlsProfileExpiresSoon

Table 376: tlsProfileExpiresSoon properties

Property name	Value
Application name	linux
Event name	tlsProfileExpiresSoon
Default severity	warning
Message format string	Certificate in TLS profile *tls_profile* expires at *expires_at_date_time*
Cause	The certificate used in the specified TLS profile will expire in the next 30 days.
Effect	Authentication using the specified TLS profile may fail once the certificate expires.

26 lldp

26.1 remotePeerAdded

Table 377: remotePeerAdded properties

Property name	Value
Application name	lldp
Event name	remotePeerAdded
Default severity	informational
Message format string	LLDP remote peer added on interface *interface_name*: System *remote_system_name* with chassis ID *remote_chassis_id*, port *remote_port_id* with MAC *remote_port_mac*
Cause	A new LLDP PDU has been received on the interface, resulting in the creation of an LLDP peer.
Effect	A new peer has been added to LLDP.

26.2 remotePeerRemoved

Table 378: remotePeerRemoved properties

Property name	Value
Application name	lldp
Event name	remotePeerRemoved
Default severity	informational
Message format string	LLDP remote peer removed on interface *interface_name*: System *remote_system_name* with chassis ID *remote_chassis_id*, port *remote_port_id* with MAC *remote_port_mac*
Cause	The TTL for the remote peer has expired without a new LLDP PDU being received.
Effect	The peer has been removed from LLDP.

26.3 remotePeerUpdated

Table 379: remotePeerUpdated properties

Property name	Value
Application name	lldp
Event name	remotePeerUpdated
Default severity	informational
Message format string	LLDP remote peer updated on interface *interface_name*: System *remote_system_name* with chassis ID *remote_chassis_id*, port *remote_port_id* with MAC *remote_port_mac*
Cause	The LLDP peer has sent new information in a LLDP PDU, without the TTL for the peer expiring.
Effect	The peer has been updated in LLDP.

27 log

27.1 bufferRollover

Table 380: bufferRollover properties

Property name	Value
Application name	log
Event name	bufferRollover
Default severity	informational
Message format string	Buffer *buffer_name* has been rolled over
Cause	The buffer has reached its configured max size, and log manager has rolled it over.
Effect	A new buffer has been opened for writing, and the old buffer has been archived. This may result in older buffers being removed from the system.

27.2 configUpdate

Table 381: configUpdate properties

Property name	Value
Application name	log
Event name	configUpdate
Default severity	informational
Message format string	Logging configuration updated
Cause	A configuration change has been made, resulting in rsyslogd configuration being regenerated.
Effect	Rsyslogd configuration has been modified, and the process has been restarted.

27.3 fileRollover

Table 382: fileRollover properties

Property name	Value
Application name	log
Event name	fileRollover
Default severity	informational
Message format string	File *file_path*/ *file_name* has been rolled over
Cause	The file has reached its configured max size, and log manager has rolled it over.
Effect	A new log file has been opened for writing, and the old log file has been archived. This may result in older logs being removed from the system.

27.4 networkNamespaceChanged

Table 383: networkNamespaceChanged properties

Property name	Value
Application name	log
Event name	networkNamespaceChanged
Default severity	informational
Message format string	Logging network namespace has changed from *old_net_namespace* to *new_net_namespace*
Cause	Configuration has been modified, resulting in the rsyslogd using the new network namespace to reach remote syslog servers.
Effect	Rsyslogd will use the new network namespace for reachability to remote syslog servers.

27.5 subsystemFacilityChanged

Table 384: subsystemFacilityChanged properties

Property name	Value
Application name	log

Property name	**Value**
Event name	subsystemFacilityChanged
Default severity	informational
Message format string	Logging output facility has changed from *old_facility* to *new_facility*
Cause	Configuration has been modified, resulting in the output facility of our subsystems changing.
Effect	Subsystems will now output logs to the newly configured facility.

28 mgmt

28.1 checkpointGenerated

Table 385: checkpointGenerated properties

Property name	Value
Application name	mgmt
Event name	checkpointGenerated
Default severity	informational
Message format string	Generated checkpoint *checkpoint_name* with comment *checkpoint_comment* on the following path *checkpoint_file_path*.
Cause	A configuration checkpoint generated on the mentioned path.
Effect	The mentioned checkpoint is stored to the filesystem.

28.2 checkpointRevertRequestReceived

Table 386: checkpointRevertRequestReceived properties

Property name	Value
Application name	mgmt
Event name	checkpointRevertRequestReceived
Default severity	warning
Message format string	Configuration is going to be reverted to checkpoint *checkpoint_id* name *checkpoint_name* comment *checkpoint_comment*.
Cause	Configuration revert request was received.
Effect	Configuration is going to be reverted to the specified checkpoint and applied to running datastore.

28.3 commitFailed

Table 387: commitFailed properties

Property name	Value
Application name	mgmt
Event name	commitFailed
Default severity	warning
Message format string	Error while committing configuration changes for user *username* session *session_id* (*message*).
Cause	Unsuccessful commit due to error(s)
Effect	Configuration changes are not applied to running datastore

28.4 commitSucceeded

Table 388: commitSucceeded properties

Property name	Value
Application name	mgmt
Event name	commitSucceeded
Default severity	informational
Message format string	All changes have been committed successfully by user *username* session *session_id*.
Cause	A successful commit
Effect	Configuration changes applied to running datastore

28.5 exclusiveConfigSessionBlockedByOtherSessionError

Table 389: exclusiveConfigSessionBlockedByOtherSessionError properties

Property name	Value
Application name	mgmt
Event name	exclusiveConfigSessionBlockedByOtherSessionError
Default severity	informational

Property name	Value
Message format string	Cannot start an exclusive configuration session for candidate name *candidate_name*, there is other configuration session in progress - session id *session_id* username *username* candidate name *candidate_name*.
Cause	Candidate datastore is locked due to other active session in progress
Effect	Exclusive configuration session Error

28.6 exclusiveConfigSessionError

Table 390: exclusiveConfigSessionError properties

Property name	Value
Application name	mgmt
Event name	exclusiveConfigSessionError
Default severity	informational
Message format string	Cannot start an exclusive configuration session, there is already another exclusive configuration session in progress - session id *session_id* username *username* candidate name *candidate_name*.
Cause	Candidate datastore is locked due to other active session in progress
Effect	Exclusive configuration session Error

28.7 privateConfigSessionError

Table 391: privateConfigSessionError properties

Property name	Value
Application name	mgmt
Event name	privateConfigSessionError
Default severity	informational
Message format string	Cannot start a configuration session for candidate name *candidate_name* by user *username*, the candidate is owned by user *candidate_username*.
Cause	Candidate datastore is owned by different user

Property name	Value
Effect	Private configuration session Error

28.8 privateSharedMismatch

Table 392: privateSharedMismatch properties

Property name	Value
Application name	mgmt
Event name	privateSharedMismatch
Default severity	informational
Message format string	Cannot start a configuration session for candidate name *candidate_name* by user *username*, cannot use private candidate with shared session or vice versa.
Cause	Candidate was created as private and the requested configuration session is shared or vice versa
Effect	Private shared configuration mismatch Error

28.9 sharedConfigSessionBlockedByOtherSessionError

Table 393: sharedConfigSessionBlockedByOtherSessionError properties

Property name	Value
Application name	mgmt
Event name	sharedConfigSessionBlockedByOtherSessionError
Default severity	informational
Message format string	Cannot start a shared configuration session for candidate name *candidate_name*, there is other configuration session in progress - session id *session_id* username *username* candidate name *candidate_name*.
Cause	Candidate datastore is locked due to other active session in progress
Effect	Shared configuration session Error

29 mirror

29.1 mirrorDestinationDelete

Table 394: mirrorDestinationDelete properties

Property name	Value
Application name	mirror
Event name	mirrorDestinationDelete
Default severity	warning
Message format string	Mirror destination *mirror_destination* is removed from configuration under mirror instance *mirror_instance_name*
Cause	Mirror destination is removed from configuration under the mentioned mirror instance
Effect	Packets will no longer be mirrorred towards the mentioned mirror destination under the mentioned mirror instance

29.2 mirrorDestinationOperDown

Table 395: mirrorDestinationOperDown properties

Property name	Value
Application name	mirror
Event name	mirrorDestinationOperDown
Default severity	critical
Message format string	Mirror destination *mirror_destination* is operationally down under mirror instance *mirror_instance_name*
Cause	Mirror destination oper state has changed from up to down the mentioned mirror instance
Effect	The oper state is down for the mentioned mirror destination under the mentioned mirror instance. Packets will no longer be mirrorred towards the mentioned mirror destination

29.3 mirrorDestinationOperUP

Table 396: mirrorDestinationOperUP properties

Property name	Value
Application name	mirror
Event name	mirrorDestinationOperUP
Default severity	warning
Message format string	Mirror destination *mirror_destination* is operationally up under mirror instance *mirror_instance_name*
Cause	Mirror destination oper state has changed from down to up the mentioned mirror instance
Effect	The oper state is up for the mentioned mirror destination under the mentioned mirror instance

29.4 mirrorDestnationAdd

Table 397: mirrorDestnationAdd properties

Property name	Value
Application name	mirror
Event name	mirrorDestnationAdd
Default severity	warning
Message format string	Mirror destination *mirror_destination* is added to configuration under mirror instance *mirror_instance_name*
Cause	Mirror destination is added in configuration under the mentioned mirror instance
Effect	Packets from mirror source(s) configured under the mentioned mirror instance will be mirrored towards the mentioned mirror destination configured under the same mirror instance if mirror instance, mirror source(s) and mirror dest are opernational up

29.5 mirrorInstanceAdminDisable

Table 398: mirrorInstanceAdminDisable properties

Property name	Value
Application name	mirror
Event name	mirrorInstanceAdminDisable
Default severity	warning
Message format string	Mirror instance *mirror_instance_name* has changed to administrative disable state
Cause	The mirror instance admin state has changed from enable to disable due to configuration change
Effect	The admin state is disable for the mentioned mirror instance

29.6 mirrorInstanceAdminEnable

Table 399: mirrorInstanceAdminEnable properties

Property name	Value
Application name	mirror
Event name	mirrorInstanceAdminEnable
Default severity	warning
Message format string	Mirror instance *mirror_instance_name* has changed to administrative enable state
Cause	The mirror instance admin state has changed from disable to enable due to configuration change
Effect	The admin state is enable for the mentioned mirror instance

29.7 mirrorInstanceOperDown

Table 400: mirrorInstanceOperDown properties

Property name	Value
Application name	mirror
Event name	mirrorInstanceOperDown

Property name	Value
Default severity	critical
Message format string	Mirror instance *mirror_instance_name* has changed to operational down state due to *oper_down_reason*
Cause	The mirror instance oper state has changed from up to down
Effect	The oper state is down on the mentioned mirror instance

29.8 mirrorInstanceOperUp

Table 401: mirrorInstanceOperUp properties

Property name	Value
Application name	mirror
Event name	mirrorInstanceOperUp
Default severity	warning
Message format string	Mirror instance *mirror_instance_name* has changed to operational up state
Cause	The mirror instance oper state has changed from down to up
Effect	The oper state is up for the mentioned mirror instance

29.9 mirrorSourceAdd

Table 402: mirrorSourceAdd properties

Property name	Value
Application name	mirror
Event name	mirrorSourceAdd
Default severity	warning
Message format string	Mirror source *mirror_source* is added to configuration under mirror instance *mirror_instance_name*
Cause	Mirror source is added in configuration under the mentioned mirror instance

Property name	Value
Effect	Packets on the mentioned mirror source will be mirrored towards the mirror destination configured under the mentioned mirror instance if mirror instance, mirror source and mirror dest are opernational up

29.10 mirrorSourceDelete

Table 403: mirrorSourceDelete properties

Property name	Value
Application name	mirror
Event name	mirrorSourceDelete
Default severity	warning
Message format string	Mirror source *mirror_source* is removed from configuration under mirror instance *mirror_instance_name*
Cause	Mirror source is removed from configuration under the mentioned mirror instance
Effect	Packets on the mentioned mirror source will no longer be mirrorred towards the mirror destination configured under the mentioned mirror instance

30 netinst

30.1 networkInstanceInterfaceDown

Table 404: networkInstanceInterfaceDown properties

Property name	Value
Application name	netinst
Event name	networkInstanceInterfaceDown
Default severity	warning
Message format string	The interface *networkinstance_interface_name* in network-instance *networkinstance_name* is now down for reason: *oper_down_reason*
Cause	This event is generated when the network instance interface has transitioned from the up state to the down state
Effect	The network instance interface is now down

30.2 networkInstanceInterfaceUp

Table 405: networkInstanceInterfaceUp properties

Property name	Value
Application name	netinst
Event name	networkInstanceInterfaceUp
Default severity	notice
Message format string	The interface *networkinstance_interface_name* in network-instance *networkinstance_name* is now up
Cause	This event is generated when the network instance interface has transitioned from the down state to the up state.
Effect	The network instance interface is now up

30.3 networkInstanceStateDown

Table 406: networkInstanceStateDown properties

Property name	Value
Application name	netinst
Event name	networkInstanceStateDown
Default severity	warning
Message format string	Network Instance *networkinstance_name* is now down
Cause	The network instance has transitioned from the up state to the down state
Effect	The network instance is now down

30.4 networkInstanceStateUp

Table 407: networkInstanceStateUp properties

Property name	Value
Application name	netinst
Event name	networkInstanceStateUp
Default severity	notice
Message format string	Network Instance *networkinstance_name* is now up
Cause	The network instance has transitioned from the down state to the up state
Effect	The network instance is now up

31 ospf

31.1 ospfAdjacencyBfdSessionSetupFailed

Table 408: ospfAdjacencyBfdSessionSetupFailed properties

Property name	Value
Application name	ospf
Event name	ospfAdjacencyBfdSessionSetupFailed
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: BFD session setup failed for the OSPF neighbor *ospfNbrRtrId*, using interface *subinterface*. Failure reason: *bfd_failure_reason*.
Cause	This event is generated when BFD session setup fails with an adjacent OSPF neighbor.
Effect	Fast failure detection may not be possible.

31.2 ospfAdjacencyChange

Table 409: ospfAdjacencyChange properties

Property name	Value
Application name	ospf
Event name	ospfAdjacencyChange
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: Adjacency with neighbor *ospfNbrRtrId*, using interface *subinterface*, moved to state *ospfNbrState* due to event *ospfNbrEvent*.
Cause	This event is generated when an OSPF Neighbor changes state.
Effect	OSPF routing information can only utilized from neighbors in an up state.

31.3 ospfAdjacencyRestartStatusChange

Table 410: ospfAdjacencyRestartStatusChange properties

Property name	Value
Application name	ospf
Event name	ospfAdjacencyRestartStatusChange
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: The graceful restart status for OSPF neighbor *ospfNbrRtrId* on interface *subinterface* moved to new state *restart_status*.
Cause	This event is generated when the graceful restart status of a neighbor changes.
Effect	None

31.4 ospfAsMaxAgeLSA

Table 411: ospfAsMaxAgeLSA properties

Property name	Value
Application name	ospf
Event name	ospfAsMaxAgeLSA
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance* area *ospfAreaId*: 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	The Max Age LSA will be flushed from the LSDB.

31.5 ospfExportLimitReached

Table 412: ospfExportLimitReached properties

Property name	Value
Application name	ospf
Event name	ospfExportLimitReached
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: The export-limit *ospfExportLimit* is reached, additional routes will not be exported by OSPF.
Cause	This event is generated when OSPF has exported the maximum number of routes.
Effect	OSPF will not export any more routes.

31.6 ospfExportLimitWarning

Table 413: ospfExportLimitWarning properties

Property name	Value
Application name	ospf
Event name	ospfExportLimitWarning
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: OSPF has reached *ospfExportLimitLogPercent*% of the export-limit *ospfExportLimit*.
Cause	This event is generated when OSPF has exported the maximum number of routes.
Effect	OSPF will not export any more routes.

31.7 ospfFailure

Table 414: ospfFailure properties

Property name	Value
Application name	ospf
Event name	ospfFailure
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: has failed due to *ospfFailureReason*.
Cause	OSPF encountered an event forcing it to go down.
Effect	OSPF goes down and will restart after a timout.

31.8 ospfIfLdpSyncStateChange

Table 415: ospfIfLdpSyncStateChange properties

Property name	Value
Application name	ospf
Event name	ospfIfLdpSyncStateChange
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: Interface *subinterface*, ldp-sync-state moved to state *ospfIfLdpSyncState*
Cause	This event is generated when an OSPF interface ldp-synchronization changes state.
Effect	Metric of the interface changes to or from infinity.

31.9 ospfIfRxBadPacket

Table 416: ospfIfRxBadPacket properties

Property name	Value
Application name	ospf
Event name	ospfIfRxBadPacket

Property name	Value
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: A bad packet was received on interface *subinterface* from *ospfPacketSrc Address* in packet type *ospfPacketType*
Cause	This event is generated An OSPF packet has been received on an interface that cannot be parsed.
Effect	Bad packet is discarded

31.10 ospfIfStateChange

Table 417: ospfIfStateChange properties

Property name	Value
Application name	ospf
Event name	ospfIfStateChange
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: Interface *subinterface*, moved to state *ospfIfState* due to event *ospf IfEvent*
Cause	This event is generated when an OSPF interface changes state.
Effect	An OSPF adjacency can not be established if the interface state is down or loop.

31.11 ospfLsdbApproachingOverflow

Table 418: ospfLsdbApproachingOverflow properties

Property name	Value
Application name	ospf
Event name	ospfLsdbApproachingOverflow
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: The number of external LSAs has exceeded 90% of the configured limit *ospfExtLsdbLimit*.

Property name	Value
Cause	The number of external LSAs in the router's link-state database has exceeded ninety percent of the configured limit.
Effect	Warning only, normal behavior will continue.

31.12 ospfLsdbOverflow

Table 419: ospfLsdbOverflow properties

Property name	Value
Application name	ospf
Event name	ospfLsdbOverflow
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: The number of external LSAs has exceeded the configured limit *ospfExt LsdbLimit*.
Cause	The number of external LSAs in the router's link-state database has exceeded the configured limit.
Effect	No additional external LSA will be added.

31.13 ospfNbrMtuMismatch

Table 420: ospfNbrMtuMismatch properties

Property name	Value
Application name	ospf
Event name	ospfNbrMtuMismatch
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: Neighbor *ospfNbrRtrId*, using interface *subinterface*, signaled an unacceptable MTU.
Cause	This event is generated when an OSPF Neighbor signals an incorrect MTU.
Effect	An OSPF adjacency cannot be established if there is an MTU mismatch.

31.14 ospfOverloadEntry

Table 421: ospfOverloadEntry properties

Property name	Value
Application name	ospf
Event name	ospfOverloadEntry
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: the LSDB database has entered the overload state due to *ospfOverload Reason*.
Cause	Overload bit configuration
Effect	No transit traffic is routed through the overloaded router.

31.15 ospfOverloadExit

Table 422: ospfOverloadExit properties

Property name	Value
Application name	ospf
Event name	ospfOverloadExit
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: the LSDB database has exited the overload state.
Cause	Overload bit cleared
Effect	The OSPF instance has cleared the overload state.

31.16 ospfOverloadWarning

Table 423: ospfOverloadWarning properties

Property name	Value
Application name	ospf

Property name	Value
Event name	ospfOverloadWarning
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: *ospfOverloadReason*.
Cause	Overload bit configuration
Effect	No transit traffic is routed through the overloaded router.

31.17 ospfSpfRunRestarted

Table 424: ospfSpfRunRestarted properties

Property name	Value
Application name	ospf
Event name	ospfSpfRunRestarted
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: SPF runs resumed - memory resources available.
Cause	There are sufficient memory resources on the system to run the SPF to completion.
Effect	OSPF stops running SPFs until enough memory resources become availableOSPF will resume running the SPFs as required.

31.18 ospfSpfRunsStopped

Table 425: ospfSpfRunsStopped properties

Property name	Value
Application name	ospf
Event name	ospfSpfRunsStopped
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: SPF runs stopped - insufficient memory resources.

Property name	Value
Cause	There are insufficient memory resources on the system to run the SPF to completion.
Effect	OSPF stops running SPFs until enough memory resources become available.

31.19 ospIfAuthDataFailure

Table 426: ospIfAuthDataFailure properties

Property name	Value
Application name	ospf
Event name	ospIfAuthDataFailure
Default severity	warning
Message format string	Network-instance *network_instance* - OSPF instance *ospfInstance*: A packet received on interface *subinterface* from *ospfPacketSrcAddress* and packet type *ospfPacketType*, failed authentication with *ospfAuth Error*
Cause	This event is caused by interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.
Effect	PDUs are dropped, with the effect depending on the PDU type

32 p4rt

32.1 globalConfigUpdate

Table 427: globalConfigUpdate properties

Property name	Value
Application name	p4rt
Event name	globalConfigUpdate
Default severity	informational
Message format string	P4RT server global configuration updated.
Cause	A global configuration change has been made, resulting in P4RT configuration being regenerated.
Effect	May result in P4RT server(s) start or stop depending on the configuration change.

32.2 networkInstanceConfigUpdate

Table 428: networkInstanceConfigUpdate properties

Property name	Value
Application name	p4rt
Event name	networkInstanceConfigUpdate
Default severity	informational
Message format string	P4RT server network instance *network_instance* configuration updated.
Cause	A configuration change has been made in the mentioned network instance, resulting in P4RT server configuration being regenerated.
Effect	May result in P4RT server start or stop depending on the configuration change.

32.3 networkInstanceP4rtOperDown

Table 429: networkInstanceP4rtOperDown properties

Property name	Value
Application name	p4rt
Event name	networkInstanceP4rtOperDown
Default severity	critical
Message format string	P4RT server in network instance *network_instance* is no longer operational.
Cause	The P4RT server in the specified network instance has transitioned from any other operational state to the down state.
Effect	P4RT is no longer available in the specified network instance.

32.4 networkInstanceP4rtOperUp

Table 430: networkInstanceP4rtOperUp properties

Property name	Value
Application name	p4rt
Event name	networkInstanceP4rtOperUp
Default severity	warning
Message format string	P4RT server in network instance *network_instance* is operational.
Cause	The P4RT server in the specified network instance has transitioned from any other operational state to the up state.
Effect	P4RT is now available in the specified network instance.

32.5 p4rtServerStart

Table 431: p4rtServerStart properties

Property name	Value
Application name	p4rt
Event name	p4rtServerStart

Property name	Value
Default severity	informational
Message format string	P4RT server started for network instance *network_instance* source address *source_address* port number *p4rt_socket*.
Cause	P4RT server has started for the mentioned network instance, source address and port number.
Effect	P4RT server is ready to receive and process requests for the mentioned network instance, source address and port number.

32.6 p4rtServerStop

Table 432: p4rtServerStop properties

Property name	Value
Application name	p4rt
Event name	p4rtServerStop
Default severity	informational
Message format string	P4RT server stopped for network *network_instance* source address *source_address* port number *p4rt_socket*.
Cause	P4RT server has stopped for the mentioned network instance, source address and port number.
Effect	P4RT server is not ready to receive and process requests for the mentioned network instance, source address and port number.

32.7 unixSocketP4rtOperDown

Table 433: unixSocketP4rtOperDown properties

Property name	Value
Application name	p4rt
Event name	unixSocketP4rtOperDown
Default severity	critical
Message format string	Unix Domain Socket P4RT server is no longer operational.

Property name	Value
Cause	The Unix domain socket P4RT server has transitioned from any other operational state to the down state.
Effect	Unix Domain Socket P4RT server is now down.

32.8 unixSocketP4rtOperUp

Table 434: unixSocketP4rtOperUp properties

Property name	Value
Application name	p4rt
Event name	unixSocketP4rtOperUp
Default severity	warning
Message format string	Unix domain socket P4RT server is operational.
Cause	The Unix domain socket P4RT server has transitioned from any other operational state to the up state.
Effect	Unix domain socket P4RT server is now up.

33 platform

33.1 airflowCorrected

Table 435: airflowCorrected properties

Property name	Value
Application name	platform
Event name	airflowCorrected
Default severity	notice
Message format string	The *type* in slot *slot* now matches the dominant airflow of other modules in the system
Cause	The specified module is now part of the majority (either front to back, or back to front) fans + PSUs in the system. This clearance is triggered when a module moves from being part of the minority to the majority, typically through other modules being plugged/unplugged.
Effect	The specified module is providing correct airflow to the system.

33.2 airflowMismatch

Table 436: airflowMismatch properties

Property name	Value
Application name	platform
Event name	airflowMismatch
Default severity	critical
Message format string	The *type* in slot *slot* does not match the airflow of other modules in the system
Cause	The inserted module does not match the airflow direction of other modules in the system.
Effect	The system is working with inefficient cooling, and may trigger thermal protection.

33.3 componentBooting

Table 437: componentBooting properties

Property name	Value
Application name	platform
Event name	componentBooting
Default severity	informational
Message format string	Component *type slot* has started initialization
Cause	The componentBooting event is generated when the active control module has started initializing the component.
Effect	The specified component has started initializing.

33.4 componentDown

Table 438: componentDown properties

Property name	Value
Application name	platform
Event name	componentDown
Default severity	critical
Message format string	Component *type slot* is no longer operational
Cause	The componentDown event is generated when a component has transitioned from any other operational state to the down state.
Effect	The specified component is now down.

33.5 componentFailed

Table 439: componentFailed properties

Property name	Value
Application name	platform
Event name	componentFailed

Property name	Value
Default severity	critical
Message format string	Component *type slot* has failed, reason *reason*
Cause	The componentFailed event is generated when a component has transitioned from any other operational state to the failed state.
Effect	The specified component is now failed.

33.6 componentInserted

Table 440: componentInserted properties

Property name	Value
Application name	platform
Event name	componentInserted
Default severity	notice
Message format string	Component *type slot* has been inserted into the system
Cause	The componentInserted event is generated when a component has been initially detected by the active control module.
Effect	The specified component is detected.

33.7 componentLocatorDisabled

Table 441: componentLocatorDisabled properties

Property name	Value
Application name	platform
Event name	componentLocatorDisabled
Default severity	notice
Message format string	Locator LED disabled on *type slot*
Cause	The componentLocatorDisabled event is generated when the locator LED for the component has been disabled, either via timeout, or via operator action.

Property name	Value
Effect	The specified component's LED is no longer flashing with locator functionality.

33.8 componentLocatorEnabled

Table 442: componentLocatorEnabled properties

Property name	Value
Application name	platform
Event name	componentLocatorEnabled
Default severity	notice
Message format string	Locator LED enabled on *type slot* for *duration* seconds
Cause	The componentLocatorEnabled event is generated when the locator LED for the component has been enabled by an operator action.
Effect	The specified component's LED is now flashing with locator functionality.

33.9 componentPowerDown

Table 443: componentPowerDown properties

Property name	Value
Application name	platform
Event name	componentPowerDown
Default severity	critical
Message format string	Component *type slot* is being powered down due to insufficient power capacity
Cause	The componentPowerDown event is generated when a component is being powered off by the active control module as a means to bring the overall power consumption of the chassis down to a level the available power supplies are able to accommodate.
Effect	The specified component is powering down.

33.10 componentPowerUp

Table 444: componentPowerUp properties

Property name	Value
Application name	platform
Event name	componentPowerUp
Default severity	warning
Message format string	Component *type slot* is being powered up due to sufficient power capacity
Cause	The componentPowerUp event is generated when a component is being powered on by the active control module, following on from a power down as a result of insufficient power supplies. This event is not generated during normal power on events.
Effect	The specified component is powering on.

33.11 componentRemoved

Table 445: componentRemoved properties

Property name	Value
Application name	platform
Event name	componentRemoved
Default severity	critical
Message format string	Component *type slot* has been removed from the system
Cause	The componentRemoved event is generated when a component has is no longer detected in the system. This does not necessarily indicate that the component has been physically removed, but indicates that it is no longer detected by the active control module.
Effect	The specified component is no longer detected by the active control module.

33.12 componentRestarted

Table 446: componentRestarted properties

Property name	Value
Application name	platform
Event name	componentRestarted
Default severity	critical
Message format string	Component *type slot* has been restarted
Cause	The componentRestarting event is generated when the a component has been restarted.
Effect	The specified component has been restarted.

33.13 componentTemperatureExceeded

Table 447: componentTemperatureExceeded properties

Property name	Value
Application name	platform
Event name	componentTemperatureExceeded
Default severity	warning
Message format string	Component *type slot* has exceeded its temperature threshold, current temperature *temperature*C
Cause	The componentTemperatureExceeded event is generated when the component has exceeded its temperature threshold.
Effect	The specified component has a temperature sensor that is overheating, the component may shut down by thermal protection.

33.14 componentTemperatureFailure

Table 448: componentTemperatureFailure properties

Property name	Value
Application name	platform
Event name	componentTemperatureFailure

Property name	Value
Default severity	warning
Message format string	Component *type slot* has exceeded its safe operating temperature, component will be powered down in 10 seconds. Current temperature *temperature*C
Cause	The componentTemperatureFailure event is generated when the component has exceeded its maximum temperature.
Effect	The specified component has a temperature sensor that has overheated, the component will shut down in 10 seconds for thermal protection.

33.15 componentTemperatureNormal

Table 449: componentTemperatureNormal properties

Property name	Value
Application name	platform
Event name	componentTemperatureNormal
Default severity	notice
Message format string	Component *type slot* temperature is now normal, current temperature *temperature*C
Cause	The componentTemperatureNormal event is generated when the component has recovered from a temperature exceeded state.
Effect	The specified component is now within temperature operating limits.

33.16 componentUp

Table 450: componentUp properties

Property name	Value
Application name	platform
Event name	componentUp
Default severity	notice
Message format string	Component *type slot* is now operational

Property name	Value
Cause	The componentUp event is generated when a component has transitioned from any other operational state to the up state.
Effect	The specified component is now up.

33.17 controlModuleActivityChange

Table 451: controlModuleActivityChange properties

Property name	Value
Application name	platform
Event name	controlModuleActivityChange
Default severity	critical
Message format string	Control module *slot* has become *activity_state*
Cause	The controlModuleActivityChange event is generated when there has been an activity change on either control module.
Effect	The specified control module has transitioned to the specified state.

33.18 controlModuleConfigSynchronized

Table 452: controlModuleConfigSynchronized properties

Property name	Value
Application name	platform
Event name	controlModuleConfigSynchronized
Default severity	informational
Message format string	Configuration synchronization with standby control module *standby_slot* has succeeded
Cause	Configuration has been successfully synchronized between the active and standby control modules.
Effect	The standby control module now has the same configuration as the active.

33.19 controlModuleImageSynchronized

Table 453: controlModuleImageSynchronized properties

Property name	Value
Application name	platform
Event name	controlModuleImageSynchronized
Default severity	informational
Message format string	Image synchronization with standby control module *standby_slot* has succeeded
Cause	Images have been successfully synchronized between the active and standby control modules.
Effect	The standby control module now has the same images as the active.

33.20 controlModuleInSync

Table 454: controlModuleInSync properties

Property name	Value
Application name	platform
Event name	controlModuleInSync
Default severity	informational
Message format string	Active and standby control modules are now synchronized
Cause	All synchronization activities have completed between the active and standby control modules.
Effect	The standby control module is now ready for a control module switchover, if necessary.

33.21 controlModuleOverlaySynchronized

Table 455: controlModuleOverlaySynchronized properties

Property name	Value
Application name	platform
Event name	controlModuleOverlaySynchronized

Property name	Value
Default severity	informational
Message format string	Overlay synchronization with standby control module *standby_slot* has succeeded
Cause	Overlays have been successfully synchronized between the active and standby control modules.
Effect	The standby control module now has the same overlay as the active.

33.22 controlModuleSyncLost

Table 456: controlModuleSyncLost properties

Property name	Value
Application name	platform
Event name	controlModuleSyncLost
Default severity	critical
Message format string	Active control module has lost visibility of the standby control module
Cause	Connection between the active and standby control modules has been lost.
Effect	The standby control module is no longer capable of taking over in the event of a failure of the active, no configuration or images are being synchronized.

33.23 controlModuleSyncStart

Table 457: controlModuleSyncStart properties

Property name	Value
Application name	platform
Event name	controlModuleSyncStart
Default severity	informational
Message format string	Active and standby control modules are now synchronizing *synchronization_category*

Property name	Value
Cause	A synchronization has been triggered between the active and standby control modules.
Effect	Configuration, images, or persistent storage is being synchronized between the active and standby control module.

33.24 fantrayEmpty

Table 458: fantrayEmpty properties

Property name	Value
Application name	platform
Event name	fantrayEmpty
Default severity	critical
Message format string	Component fan-tray *slot* is not present in the system
Cause	The fantrayEmpty event is generated when a fan-tray has transitioned from any other operational state to the empty state, or is never present.
Effect	The system may have cooling issues.

33.25 linecardCapacityDegraded

Table 459: linecardCapacityDegraded properties

Property name	Value
Application name	platform
Event name	linecardCapacityDegraded
Default severity	critical
Message format string	Linecard *slot* forwarding complex *forwarding-complex* fabric capacity degraded
Cause	The specified linecard's forwarding complex has insufficient operational fabric links.
Effect	Packets may be dropped if the linecard's forwarding complex is sending and receiving significant amounts of traffic to the fabric.

33.26 linecardCapacityNormal

Table 460: linecardCapacityNormal properties

Property name	Value
Application name	platform
Event name	linecardCapacityNormal
Default severity	informational
Message format string	Linecard *slot* forwarding complex *forwarding-complex* fabric capacity normal
Cause	The specified linecard's forwarding complex has sufficient operational fabric links again.
Effect	Normal behavior is restored for sending and receiving traffic to the fabric.

33.27 platformLowPower

Table 461: platformLowPower properties

Property name	Value
Application name	platform
Event name	platformLowPower
Default severity	emergency
Message format string	Insufficient power for currently installed components, *current_power*W available, *required_power*W required
Cause	Available power from operational power supplies is insufficient to power all components in the system.
Effect	Components in the system will be powered down until required power is lower than what is supplied by operational power supplies.

33.28 platformLowReservePower

Table 462: platformLowReservePower properties

Property name	Value
Application name	platform
Event name	platformLowReservePower
Default severity	critical
Message format string	Insufficient reserve power for currently installed components, *current_power*W available, *required_power*W required
Cause	Available power is less than one power supply capacity extra to power all components in the system.
Effect	Power will be insufficient if one operational power supply is lost.

33.29 platformNoPowerRedundancy

Table 463: platformNoPowerRedundancy properties

Property name	Value
Application name	platform
Event name	platformNoPowerRedundancy
Default severity	warning
Message format string	Power redundancy based on mode *redundancy_mode* is not available, required PSUs *required_psus*, operational PSUs *active_psus*
Cause	The available PSUs are not able to accomodate the configured power redundancy mode.
Effect	The desired power redundancy is not available.

33.30 platformNormalPower

Table 464: platformNormalPower properties

Property name	Value
Application name	platform
Event name	platformNormalPower

Property name	Value
Default severity	informational
Message format string	Sufficient power for currently installed components, *current_power*W available, *required_power*W required
Cause	Available power from operational power supplies is sufficient to power all components in the system.
Effect	Enough power is available.

33.31 platformPowerRedundancyRecovered

Table 465: platformPowerRedundancyRecovered properties

Property name	Value
Application name	platform
Event name	platformPowerRedundancyRecovered
Default severity	informational
Message format string	Power redundancy based on mode *redundancy_mode* is available, required PSUs *required_psus*, operational PSUs *active_psus*
Cause	The available PSUs are able to accomodate the configured power redundancy mode.
Effect	The desired power redundancy is available.

33.32 psuInputDown

Table 466: psuInputDown properties

Property name	Value
Application name	platform
Event name	psuInputDown
Default severity	warning
Message format string	Power input on power-supply *slot* is down
Cause	Input fault on the specified power supply is set.
Effect	The specified power supply can no longer supply power to the system.

33.33 psuInputUp

Table 467: psuInputUp properties

Property name	Value
Application name	platform
Event name	psuInputUp
Default severity	notice
Message format string	Power input on power-supply *slot* is up
Cause	Input fault on the specified power supply is clear.
Effect	The specified power supply can now supply power to the system.

33.34 psuOutputDown

Table 468: psuOutputDown properties

Property name	Value
Application name	platform
Event name	psuOutputDown
Default severity	warning
Message format string	Power output on power-supply *slot* is down
Cause	Output fault on the specified power supply is set.
Effect	The specified power supply can no longer supply power to the system.

33.35 psuOutputUp

Table 469: psuOutputUp properties

Property name	Value
Application name	platform
Event name	psuOutputUp
Default severity	notice

Property name	Value
Message format string	Power output on power-supply *slot* is up
Cause	Output fault on the specified power supply is clear.
Effect	The specified power supply can now supply power to the system.

33.36 psuTemperatureFault

Table 470: psuTemperatureFault properties

Property name	Value
Application name	platform
Event name	psuTemperatureFault
Default severity	warning
Message format string	Component *type slot* has raised a temperature fault, current temperature *temperature*C
Cause	The psuTemperatureFault event is generated when the power supply raises a temperature fault.
Effect	The power supply is overheating, and may shut down by thermal protection.

33.37 psuTemperatureNormal

Table 471: psuTemperatureNormal properties

Property name	Value
Application name	platform
Event name	psuTemperatureNormal
Default severity	notice
Message format string	Component *type slot* temperature fault is now clear, current temperature *temperature*C
Cause	The psuTemperatureNormal event is generated when the power supply recovered from a temperature fault state.
Effect	The power supply is now within temperature operating limits.

33.38 systemInServiceSoftwareUpgrade

Table 472: systemInServiceSoftwareUpgrade properties

Property name	Value
Application name	platform
Event name	systemInServiceSoftwareUpgrade
Default severity	critical
Message format string	System is upgrading from *old_version* to *new_version*, utilizing warm reboot
Cause	The systemInServiceSoftwareUpgrade event is generated when a software triggered in service software upgrade request has been made.
Effect	The control and management plane of the system will go offline, the datapath will continue forwarding based on current state. The system will upgrade the kernel, operating system, and/or applications as needed.

33.39 systemReboot

Table 473: systemReboot properties

Property name	Value
Application name	platform
Event name	systemReboot
Default severity	critical
Message format string	System going down for reboot
Cause	The systemReboot event is generated when a software triggered reboot has been made.
Effect	The system will go offline for reboot.

33.40 systemWarmReboot

Table 474: systemWarmReboot properties

Property name	Value
Application name	platform
Event name	systemWarmReboot
Default severity	critical
Message format string	System going down for warm reboot
Cause	The systemWarmReboot event is generated when a software triggered warm reboot has been made.
Effect	The control and management plane of the system will go offline, the datapath will continue forwarding based on current state.

33.41 systemWarmRebootAborted

Table 475: systemWarmRebootAborted properties

Property name	Value
Application name	platform
Event name	systemWarmRebootAborted
Default severity	critical
Message format string	System has aborted a requested warm reboot due to *reason*
Cause	The systemWarmRebootAborted event is generated when a software triggered warm reboot request has been aborted, typically due to unsupported configuration.
Effect	The in progress warm reboot has been aborted, no effect to system configuration or state.

34 qos

34.1 platformQoSProfileHighUtilization

Table 476: platformQoSProfileHighUtilization properties

Property name	Value
Application name	qos
Event name	platformQoSProfileHighUtilization
Default severity	warning
Message format string	The QoS resource called *resource-name* has reached *threshold*% or more utilization on linecard *linecard*, forwarding complex *forwarding-complex*. Only *free-entries* entries are remaining.
Cause	This event is generated when the utilization of a QoS resource has increased to a level that may warrant concern if futher resources are consumed
Effect	None

34.2 platformQoSProfileHighUtilizationLowered

Table 477: platformQoSProfileHighUtilizationLowered properties

Property name	Value
Application name	qos
Event name	platformQoSProfileHighUtilizationLowered
Default severity	notice
Message format string	The QoS resource called *resource-name* has decreased back to *threshold*% or less utilization on linecard *linecard*, forwarding complex *forwarding-complex*.
Cause	This event is generated when the utilization of a QoS resource has decreased to a level that may no longer warrant concern
Effect	None

35 ra_guard-agent

35.1 ra_guardAdd

Table 478: ra_guardAdd properties

Property name	Value
Application name	ra_guard-agent
Event name	ra_guardAdd
Default severity	notice
Message format string	RA Guard Policy *pol-name* associated with subinterface *if-name*, VLAN *vlan*
Cause	This notification is generated when an RA policy is added to a subinterface.
Effect	The associated RA Policy is now applied to the subinterface.

35.2 ra_guardRemove

Table 479: ra_guardRemove properties

Property name	Value
Application name	ra_guard-agent
Event name	ra_guardRemove
Default severity	notice
Message format string	RA Guard Policy *pol-name* removed from subinterface *if-name*, VLAN *vlan*
Cause	This notification is generated when an RA policy is removed from a subinterface.
Effect	An RA Policy is no longer associated with the specified subinterface.

36 sflow

36.1 sFlowAgentChange

Table 480: sFlowAgentChange properties

Property name	Value
Application name	sflow
Event name	sFlowAgentChange
Default severity	notice
Message format string	SFLOW: The global sFlow Agent has administratively been changed to *state*
Cause	This notification is generated when a sFlow global process changes administrative state.
Effect	The sFlow global process state has changed.

36.2 sFlowCollectorUnreachable

Table 481: sFlowCollectorUnreachable properties

Property name	Value
Application name	sflow
Event name	sFlowCollectorUnreachable
Default severity	warning
Message format string	SFLOW: Collector *collector-id* - IP address: *collector-ip* is unreachable
Cause	This notification is generated when the specified sFlow collector will no longer receive sflow sample data until reachability is restored
Effect	Restore IP reachability to the sFlow collector.

37 sync

37.1 syncFreqClockQLChange

Table 482: syncFreqClockQLChange properties

Property name	Value
Application name	sync
Event name	syncFreqClockQLChange
Default severity	notice
Message format string	The system frequency clock's Quality Level (ql) has transitioned to *freq_clock_ql*
Cause	This notification is generated when a frequency clock transitions to a new ql.
Effect	The system's frequency clock is synced to remote clock with this ql.

37.2 syncFreqClockRefChange

Table 483: syncFreqClockRefChange properties

Property name	Value
Application name	sync
Event name	syncFreqClockRefChange
Default severity	notice
Message format string	The system frequency clock reference has transitioned to frequency reference instance *instance_number*
Cause	This notification is generated when a frequency reference instance selected has changed.
Effect	The system frequency clock will follow the new reference.

37.3 syncFreqClockStateChange

Table 484: syncFreqClockStateChange properties

Property name	Value
Application name	sync
Event name	syncFreqClockStateChange
Default severity	notice
Message format string	The system frequency clock state has transitioned to *freq_clock_state*
Cause	This notification is generated when a frequency clock transitions to a new state.
Effect	The system's frequency clock behavior is based on this state.

37.4 syncFreqInstanceAlarmChange

Table 485: syncFreqInstanceAlarmChange properties

Property name	Value
Application name	sync
Event name	syncFreqInstanceAlarmChange
Default severity	notice
Message format string	Frequency reference instance *instance_number*: The alarm state has transitioned to *alarm_state*
Cause	This notification is generated when a frequency Reference instance transitions to a new alarm state.
Effect	If there is an alarm for a frequency reference instance, it will not be qualified for use.

37.5 syncFreqInstanceQLChange

Table 486: syncFreqInstanceQLChange properties

Property name	Value
Application name	sync
Event name	syncFreqInstanceQLChange

Property name	Value
Default severity	notice
Message format string	Frequency reference instance *instance_number*: The Quality Level (ql) has transitioned to *ql_number*
Cause	This notification is generated when a frequency reference Instance transitions to a new QL.
Effect	The new QL will be taken into account when for system frequency clock reference selection if ql-selection is set.

37.6 syncPTPParentChange

Table 487: syncPTPParentChange properties

Property name	Value
Application name	sync
Event name	syncPTPParentChange
Default severity	notice
Message format string	PTP has transitioned to new parent *parent_clock_mac_address* on port *parent_clock_port* with clockClass of *parent_clockclass*.
Cause	This notification is generated when the PTP clock transitions to a new parent.
Effect	The ptp clock will follow this new parent clock.

37.7 syncPTPParentChangeIP

Table 488: syncPTPParentChangeIP properties

Property name	Value
Application name	sync
Event name	syncPTPParentChangeIP
Default severity	notice
Message format string	PTP has transitioned to new parent *parent_clock_ip* in routing instance *parent_clock_router* with clockClass of *parent_clockclass*.

Property name	Value
Cause	This notification is generated when the PTP clock transitions to a new IP parent.
Effect	The ptp clock will follow this new parent clock.

37.8 syncPTPPortPTSFUnusable

Table 489: syncPTPPortPTSFUnusable properties

Property name	Value
Application name	sync
Event name	syncPTPPortPTSFUnusable
Default severity	warning
Message format string	PTP detected excessive noise between PTP port number *ptp_neighbor_port_number* and parent clock ID *ptp_neighbor_clock_id*.
Cause	The PTP process detected excessive noise between the local port and the indicated external Master port.
Effect	Any Announce messages received from the indicated neighbor shall be excluded from the BMCA algorithm until this condition is cleared.

37.9 syncPTPTimeRecoveryState

Table 490: syncPTPTimeRecoveryState properties

Property name	Value
Application name	sync
Event name	syncPTPTimeRecoveryState
Default severity	notice
Message format string	PTP has transitioned to time recovery state of *ptp_time_rec_state*
Cause	This notification is generated when the PTP clock transitions to a new time recovery state.
Effect	The ptp clock's tim recovery behavior will be based on this state.

Customer document and product support

Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback