NOKIA

Nokia Service Router Linux

LOG EVENTS GUIDE
RELEASE 21.11

3HE 17909 AAAA TQZZA
Issue 1

December 2021

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

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

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

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

No part of this document may be modified.

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

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.

1.1 What's new

See the Log event change summary for a list of log events that have been added or removed.

1.2 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.

1.3 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**

- Angle brackets (< >) indicate an item that is not used verbatim. For example, for the command show **ethernet <name>**, **name** should be replaced with the name of the interface.
- 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 Log events

The sections that follow define supported log events.

Reference the Log event change summary below for a summary of log event changes since this document was last published.

3.1 Log event change summary

Event Name	Change
evpnAutoDiscoveryEviRouteAddDroppedDueToUnexpectedEthTag	New
evpnAutoDiscoveryEviRouteWithdrawDroppedDueToUnexpectedEthTag	New
evpnInclMcastRouteAddDroppedDueToUnexpectedEthTag	New
evpnInclMcastRouteWithdrawDroppedDueToUnexpectedEthTag	New
evpnMacRouteAddDroppedDueToUnexpectedEthTag	New
evpnMacRouteWithdrawDroppedDueToUnexpectedEthTag	New
isisLdpSyncExited	New
isisLdpSyncTimerStarted	New
ldpInterfaceDown	New
ldpInterfaceUp	New
ldpIpv4InstanceDown	New
ldpIpv4InstanceUp	New
ldpSessionDown	New
ldpSessionFecLimitReached	New
ldpSessionLocalIPv4Overload	New
ldpSessionPeerIPv4Overload	New
ldpSessionUp	New
networkInstanceBridgeTableProxyArpDuplicateIpAddressDeleted	New

Event Name	Change
networkInstanceBridgeTableProxyArpDuplicateIpAddressDetected	New
networkInstanceBridgeTableProxyArpLimitHighUtilization	New
networkInstanceBridgeTableProxyArpLimitHighUtilizationLowered	New
systemBridgeTableProxyArpLimitHighUtilization	New
systemBridgeTableProxyArpLimitHighUtilizationLowered	New

3.2 aaa

3.2.1 serverDown

Table 4: 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.

3.2.2 serverGroupDown

Table 5: serverGroupDown properties

Property name	Value
Application name	aaa
Event name	serverGroupDown
Default severity	critical

Property name	Value
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.

3.2.3 serverRouteUnavailable

Table 6: 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.

3.2.4 serverTimeout

Table 7: 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.

Property name	Value
Effect	The specified server can no longer be used for authentication, authorization, or accounting transactions.

3.2.5 sessionClosed

Table 8: 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.

3.2.6 sessionDisconnected

Table 9: 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.

3.2.7 sessionOpened

Table 10: sessionOpened properties

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

3.2.8 userAuthenticationFailed

Table 11: 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.

3.2.9 userAuthenticationSucceeded

Table 12: userAuthenticationSucceeded properties

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

Property name	Value
Message format string	User **user_name** successfully authenticated from host **remote_host**
Cause	The specified user has successfully authenticated.
Effect	None.

3.3 acl

3.3.1 aclCpmIpv4MatchedPacket

Table 13: 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

3.3.2 aclCpmIpv6MatchedPacket

Table 14: 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

Property name	Value
	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

3.3.3 aclInterfaceInputIpv4MatchedPacket

Table 15: 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

3.3.4 aclInterfaceInputIpv6MatchedPacket

Table 16: 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**)

Property name	Value
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

3.3.5 aclInterfaceOutputIpv4MatchedPacket

Table 17: 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

3.3.6 aclInterfaceOutputIpv6MatchedPacket

Table 18: 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**)

Property name	Value
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

3.3.7 aclTcamProgComplete

Table 19: 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

3.3.8 platformAclHighUtilization

Table 20: 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

Property name	Value
Effect	None

3.3.9 platformAclHighUtilizationLowered

Table 21: 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

3.3.10 platformTcamHighUtilization

Table 22: 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

3.3.11 platformTcamHighUtilizationLowered

Table 23: 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

3.4 arpnd

3.4.1 ipArpEntryUpdated

Table 24: 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

3.4.2 ipSubinterfaceDuplicateIpv4Address

Table 25: 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

3.4.3 ipSubinterfaceDuplicateIpv6Address

Table 26: 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

3.4.4 ipSubinterfaceDuplicateMacAddress

Table 27: ipSubinterfaceDuplicateMacAddress properties

Property name	Value
Application name	arpnd

Property name	Value
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

3.4.5 ipSubinterfaceInvalidArp

Table 28: ipSubinterfaceInvalidArp properties

Property name	Value
Application name	arpnd
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

3.4.6 ipSubinterfaceInvalidIpv6NeighborSolicitation

Table 29: 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.

Property name	Value
Cause	This event is generated when IPv6 neighbor discovery receives a NS message for an invalid IPv6 address
Effect	None

3.4.7 ipv6NeighborEntryUpdated

Table 30: 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**.
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

3.5 bfd

3.5.1 bfdDownEvent

Table 31: 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-**

Property name	Value
	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 sessions transitions to the Down or Admin Down state from an Up state.
Effect	The specified BFD sessions is now down. If the new state is Down, the session is 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.

3.5.2 bfdMaxSessionActive

Table 32: 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.
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.

3.5.3 bfdProtocolClientAdd

Table 33: bfdProtocolClientAdd properties

Property name	Value
Application name	bfd
Event name	bfdProtocolClientAdd

Property name	Value
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.

3.5.4 bfdProtocolClientRemove

Table 34: 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
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

3.5.5 bfdSessionDeleted

Table 35: bfdSessionDeleted properties

Property name	Value
Application name	bfd
Event name	bfdSessionDeleted
Default severity	notice

Property name	Value
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.

3.5.6 bfdSessionUp

Table 36: 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 sessions transitions to the up state.
Effect	The BFD session is now operational.

3.5.7 microbfdDownEvent

Table 37: microbfdDownEvent properties

Property name	Value
Application name	bfd
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

Property name	Value
	remote-diagnostic code: **remote-diagnostic-str** (**remote-diagnostic-code**)
Cause	This notification is generated when a BFD sessions transitions to the Down or Admin Down state from an Up state.
Effect	The specified BFD sessions is now down. If the new state is Down, the session is 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.

3.5.8 microbfdMaxSessionActive

Table 38: 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.

3.5.9 microbfdSessionDeleted

Table 39: microbfdSessionDeleted properties

Property name	Value
Application name	bfd
Event name	microbfdSessionDeleted
Default severity	notice

Property name	Value
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.

3.5.10 microbfdSessionUp

Table 40: 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 sessions transitions to the up state.
Effect	The BFD session is now operational.

3.6 bgp

3.6.1 bgpIncomingDynamicPeerLimitReached

Table 41: bgpIncomingDynamicPeerLimitReached properties

Property name	Value
Application name	bgp
Event name	bgpIncomingDynamicPeerLimitReached
Default severity	notice

Property name	Value
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.

3.6.2 bgpInstanceConvergenceStateTransition

Table 42: 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

3.6.3 bgpLowMemory

Table 43: 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.

Property name	Value
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.

3.6.4 bgpNeighborBackwardTransition

Table 44: 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.

3.6.5 bgpNeighborClosedTCPConn

Table 45: 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.

3.6.6 bgpNeighborEstablished

Table 46: bgpNeighborEstablished properties

Property name	Value
Application name	bgp
Event name	bgpNeighborEstablished
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.

3.6.7 bgpNeighborGRHelpingStarted

Table 47: 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.

3.6.8 bgpNeighborGRHelpingStopped

Table 48: bgpNeighborGRHelpingStopped properties

Property name	Value
Application name	bgp

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

3.6.9 bgpNeighborHoldTimeExpired

Table 49: 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.

3.6.10 bgpNeighborInvalidLocalIP

Table 50: bgpNeighborInvalidLocalIP properties

Property name	Value
Application name	bgp
Event name	bgpNeighborInvalidLocalIP
Default severity	warning

Property name	Value
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.

3.6.11 bgpNeighborNoOpenReceived

Table 51: 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.

3.6.12 bgpNeighborPrefixLimitReached

Table 52: 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.

Property name	Value
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.

3.6.13 bgpNeighborPrefixLimitThresholdReached

Table 53: 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.

3.6.14 bgpNeighborUnknownRemoteIP

Table 54: 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.

Property name	Value
Effect	No routes can be exchanged with this peer.

3.6.15 bgpNLRIInvalid

Table 55: 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.

3.6.16 bgpNotificationReceivedFromNeighbor

Table 56: 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.

3.6.17 bgpNotificationSentToNeighbor

Table 57: 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.

3.6.18 bgpOutgoingDynamicPeerLimitReached

Table 58: 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.

3.6.19 bgpPathAttributeDiscarded

Table 59: 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.

3.6.20 bgpPathAttributeMalformed

Table 60: 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.

3.6.21 bgpRouteWithdrawnDueToError

Table 61: 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.

3.6.22 bgpUpdateInvalid

Table 62: 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.

3.7 bridgetable

3.7.1 l2SubinterfaceBridgeTableDuplicateMacAddressDeleted

Table 63: 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.

3.7.2 l2SubinterfaceBridgeTableDuplicateMacAddressDetected

Table 64: 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

3.7.3 l2SubinterfaceBridgeTableMacLimitHighUtilization

Table 65: 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

3.7.4 l2SubinterfaceBridgeTableMacLimitHighUtilizationLowered

Table 66: 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

3.7.5 l2SubinterfaceBridgeTableMacLimitLowered

Table 67: 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.

3.7.6 l2SubinterfaceBridgeTableMacLimitReached

Table 68: 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.

3.7.7 networkInstanceBridgeTableDuplicateMacAddressDeleted

Table 69: 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.

3.7.8 networkInstanceBridgeTableDuplicateMacAddressDetected

Table 70: 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

3.7.9 networkInstanceBridgeTableMacLimitHighUtilization

Table 71: 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

3.7.10 networkInstanceBridgeTableMacLimitHighUtilizationLowered

Table 72: 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

3.7.11 networkInstanceBridgeTableMacLimitLowered

Table 73: 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.

3.7.12 networkInstanceBridgeTableMacLimitReached

Table 74: 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.

3.7.13 networkInstanceBridgeTableProxyArpDuplicateIpAddressDeleted

Table 75: networkInstanceBridgeTableProxyArpDuplicateIpAddressDeleted properties

Property name	Value
Application name	bridgetable

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

3.7.14 networkInstanceBridgeTableProxyArpDuplicateIpAddressDetected

Table 76: networkInstanceBridgeTableProxyArpDuplicateIpAddressDetected properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyArpDuplicateIpAddressDetected
Default severity	notice
Message format string	A duplicate link-layer-address **new-mac-address** was detected for proxy ARP 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 ARP IP on the network-instance.
Effect	A traffic disruption may occur if both systems are active

3.7.15 networkInstanceBridgeTableProxyArpLimitHighUtilization

Table 77: networkInstanceBridgeTableProxyArpLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	networkInstanceBridgeTableProxyArpLimitHighUtilization
Default severity	warning

Property name	Value
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

3.7.16 networkInstanceBridgeTableProxyArpLimitHighUtilizationLowered

Table 78: 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

3.7.17 systemBridgeTableMacLimitHighUtilization

Table 79: systemBridgeTableMacLimitHighUtilization properties

Property name	Value
Application name	bridgetable
Event name	systemBridgeTableMacLimitHighUtilization
Default severity	warning

Property name	Value
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**.
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

3.7.18 systemBridgeTableMacLimitHighUtilizationLowered

Table 80: 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

3.7.19 systemBridgeTableMacLimitLowered

Table 81: 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**.

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

3.7.20 systemBridgeTableMacLimitReached

Table 82: 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.

3.7.21 systemBridgeTableProxyArpLimitHighUtilization

Table 83: 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

3.7.22 systemBridgeTableProxyArpLimitHighUtilizationLowered

Table 84: 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

3.7.23 vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilization

Table 85: 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

3.7.24 vxlanInterfaceBridgeTableMulticastDestinationsLimitHighUtilizationLowered

Table 86: 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

3.7.25 vxlanInterfaceBridgeTableMulticastDestinationsLimitLowered

Table 87: 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.

3.7.26 vxlanInterfaceBridgeTableMulticastDestinationsLimitReached

Table 88: 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.

3.8 chassis

3.8.1 platformDatapathResourceHighUtilization

Table 89: 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

3.8.2 platformDatapathResourceHighUtilizationLowered

Table 90: 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

3.8.3 platformDatapathResourceLimitCleared

Table 91: 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

3.8.4 platformDatapathResourceLimitReached

Table 92: 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

3.8.5 platformMtuHighUtilization

Table 93: 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

3.8.6 platformMtuHighUtilizationLowered

Table 94: 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

3.8.7 platformPipelineResourceHighUtilization

Table 95: 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

3.8.8 platformPipelineResourceHighUtilizationLowered

Table 96: 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

3.8.9 platformPipelineResourceLimitCleared

Table 97: 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

3.8.10 platformPipelineResourceLimitReached

Table 98: 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

3.8.11 portDown

Table 99: 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

3.8.12 portUp

Table 100: portUp properties

Property name	Value
Application name	chassis

Property name	Value
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

3.8.13 subinterfaceDown

Table 101: 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

3.8.14 subinterfaceUp

Table 102: 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.

Property name	Value
Effect	The subinterface is now up

3.8.15 transceiverChannelHighInputPowerAlarm

Table 103: 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

3.8.16 transceiverChannelHighInputPowerAlarmClear

Table 104: transceiverChannelHighInputPowerAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighInputPowerAlarmClear
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

3.8.17 transceiverChannelHighInputPowerWarning

Table 105: 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

3.8.18 transceiverChannelHighInputPowerWarningClear

Table 106: 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
Effect	High input power may affect transceiver performance

3.8.19 transceiverChannelHighLaserBiasCurrentAlarm

Table 107: transceiverChannelHighLaserBiasCurrentAlarm properties

Property name	Value
Application name	chassis

Property name	Value
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

3.8.20 transceiverChannelHighLaserBiasCurrentAlarmClear

Table 108: 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

3.8.21 transceiverChannelHighLaserBiasCurrentWarning

Table 109: transceiverChannelHighLaserBiasCurrentWarning properties

Property name	Value
Application name	chassis
Event name	transceiverChannelHighLaserBiasCurrentWarning
Default severity	warning

Property name	Value
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

3.8.22 transceiverChannelHighLaserBiasCurrentWarningClear

Table 110: 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

3.8.23 transceiverChannelHighOutputPowerAlarm

Table 111: transceiverChannelHighOutputPowerAlarm properties

Property name	Value
Application name	chassis
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

Property name	Value
Effect	High output power may affect transceiver performance

3.8.24 transceiverChannelHighOutputPowerAlarmClear

Table 112: 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

3.8.25 transceiverChannelHighOutputPowerWarning

Table 113: 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
Cause	The output power of the optical channel has increased
Effect	High output power may affect transceiver performance

3.8.26 transceiverChannelHighOutputPowerWarningClear

Table 114: 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

3.8.27 transceiverChannelLowInputPowerAlarm

Table 115: 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

3.8.28 transceiverChannelLowInputPowerAlarmClear

Table 116: transceiverChannelLowInputPowerAlarmClear properties

Property name	Value
Application name	chassis

Property name	Value
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

3.8.29 transceiverChannelLowInputPowerWarning

Table 117: 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

3.8.30 transceiverChannelLowInputPowerWarningClear

Table 118: transceiverChannelLowInputPowerWarningClear properties

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

Property name	Value
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

3.8.31 transceiverChannelLowLaserBiasCurrentAlarm

Table 119: 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

3.8.32 transceiverChannelLowLaserBiasCurrentAlarmClear

Table 120: 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

3.8.33 transceiverChannelLowLaserBiasCurrentWarning

Table 121: 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

3.8.34 transceiverChannelLowLaserBiasCurrentWarningClear

Table 122: 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

3.8.35 transceiverChannelLowOutputPowerAlarm

Table 123: 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

3.8.36 transceiverChannelLowOutputPowerAlarmClear

Table 124: 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

3.8.37 transceiverChannelLowOutputPowerWarning

Table 125: transceiverChannelLowOutputPowerWarning properties

Property name	Value
Application name	chassis

Property name	Value
Event name	transceiverChannelLowOutputPowerWarning
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

3.8.38 transceiverChannelLowOutputPowerWarningClear

Table 126: 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

3.8.39 transceiverHighInputPowerAlarm

Table 127: 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

Property name	Value
Cause	The input power of the optics has increased
Effect	High input power may affect transceiver performance

3.8.40 transceiverHighInputPowerAlarmClear

Table 128: 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

3.8.41 transceiverHighInputPowerWarning

Table 129: 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

3.8.42 transceiverHighInputPowerWarningClear

Table 130: 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

3.8.43 transceiverHighLaserBiasCurrentAlarm

Table 131: 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

3.8.44 transceiverHighLaserBiasCurrentAlarmClear

Table 132: transceiverHighLaserBiasCurrentAlarmClear properties

Property name	Value
Application name	chassis

Property name	Value
Event name	transceiverHighLaserBiasCurrentAlarmClear
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

3.8.45 transceiverHighLaserBiasCurrentWarning

Table 133: 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

3.8.46 transceiverHighLaserBiasCurrentWarningClear

Table 134: 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

Property name	Value
Cause	Laser bias current has decreased
Effect	High laser bias may affect transceiver performance

3.8.47 transceiverHighOutputPowerAlarm

Table 135: 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

3.8.48 transceiverHighOutputPowerAlarmClear

Table 136: 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

3.8.49 transceiverHighOutputPowerWarning

Table 137: transceiverHighOutputPowerWarning properties

Property name	Value
Application name	chassis
Event name	transceiverHighOutputPowerWarning
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

3.8.50 transceiverHighOutputPowerWarningClear

Table 138: 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

3.8.51 transceiverLowInputPowerAlarm

Table 139: transceiverLowInputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverLowInputPowerAlarm

Property name	Value
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

3.8.52 transceiverLowInputPowerAlarmClear

Table 140: 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

3.8.53 transceiverLowInputPowerWarning

Table 141: 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

3.8.54 transceiverLowInputPowerWarningClear

Table 142: transceiverLowInputPowerWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowInputPowerWarningClear
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

3.8.55 transceiverLowLaserBiasCurrentAlarm

Table 143: 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

3.8.56 transceiverLowLaserBiasCurrentAlarmClear

Table 144: transceiverLowLaserBiasCurrentAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverLowLaserBiasCurrentAlarmClear

Property name	Value
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

3.8.57 transceiverLowLaserBiasCurrentWarning

Table 145: 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

3.8.58 transceiverLowLaserBiasCurrentWarningClear

Table 146: 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

3.8.59 transceiverLowOutputPowerAlarm

Table 147: transceiverLowOutputPowerAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverLowOutputPowerAlarm
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

3.8.60 transceiverLowOutputPowerAlarmClear

Table 148: 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

3.8.61 transceiverLowOutputPowerWarning

Table 149: transceiverLowOutputPowerWarning properties

Property name	Value
Application name	chassis

Property name	Value
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

3.8.62 transceiverLowOutputPowerWarningClear

Table 150: 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

3.8.63 transceiverModuleDown

Table 151: 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

Property name	Value
Cause	The transceiver oper-state has transitioned from the up state to any lower state
Effect	The transceiver is not operational

3.8.64 transceiverModuleHighTemperatureAlarm

Table 152: transceiverModuleHighTemperatureAlarm properties

Property name	Value
Application name	chassis
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

3.8.65 transceiverModuleHighTemperatureAlarmClear

Table 153: 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

3.8.66 transceiverModuleHighTemperatureWarning

Table 154: 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
Effect	High temperatures may affect transceiver performance

3.8.67 transceiverModuleHighTemperatureWarningClear

Table 155: 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

3.8.68 transceiverModuleHighVoltageAlarm

Table 156: transceiverModuleHighVoltageAlarm properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighVoltageAlarm

Property name	Value
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

3.8.69 transceiverModuleHighVoltageAlarmClear

Table 157: 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

3.8.70 transceiverModuleHighVoltageWarning

Table 158: 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

3.8.71 transceiverModuleHighVoltageWarningClear

Table 159: transceiverModuleHighVoltageWarningClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleHighVoltageWarningClear
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

3.8.72 transceiverModuleLowTemperatureAlarm

Table 160: 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

3.8.73 transceiverModuleLowTemperatureAlarmClear

Table 161: transceiverModuleLowTemperatureAlarmClear properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowTemperatureAlarmClear

Property name	Value
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

3.8.74 transceiverModuleLowTemperatureWarning

Table 162: 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

3.8.75 transceiverModuleLowTemperatureWarningClear

Table 163: 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

3.8.76 transceiverModuleLowVoltageAlarm

Table 164: transceiverModuleLowVoltageAlarm properties

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

3.8.77 transceiverModuleLowVoltageAlarmClear

Table 165: 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

3.8.78 transceiverModuleLowVoltageWarning

Table 166: transceiverModuleLowVoltageWarning properties

Property name	Value
Application name	chassis
Event name	transceiverModuleLowVoltageWarning

Property name	Value
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

3.8.79 transceiverModuleLowVoltageWarningClear

Table 167: 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

3.8.80 transceiverModuleUp

Table 168: 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

Property name	Value
Effect	The transceiver is now operational

3.9 debug

3.9.1 setAllConfigLevels

Table 169: 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.

3.9.2 setAllStartupLevels

Table 170: 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.

3.9.3 setHighBaselineLogLevels

Table 171: 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.

3.10 dhcp

3.10.1 dhcp6ClientAddressDeclined

Table 172: 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

3.10.2 dhcp6ClientIpv6AddressValidLifetimeExpired

Table 173: 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

3.10.3 dhcp6ClientRebindAttempted

Table 174: 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

3.10.4 dhcp6ClientReconfigureMsgDropped

Table 175: dhcp6ClientReconfigureMsgDropped properties

Property name	Value
Application name	dhcp

Property name	Value
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

3.10.5 dhcp6ClientRenewSuccess

Table 176: 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

3.10.6 dhcpClientAddressDeclined

Table 177: dhcpClientAddressDeclined properties

Property name	Value
Application name	dhcp
Event name	dhcpClientAddressDeclined
Default severity	notice

Property name	Value
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

3.10.7 dhcpClientLeaseExpired

Table 178: 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

3.10.8 dhcpClientRebindAttempted

Table 179: 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

Property name	Value
Effect	The lease may expire if the rebind is not successful

3.10.9 dhcpClientRenewSuccess

Table 180: dhcpClientRenewSuccess properties

Property name	Value
Application name	dhcp
Event name	dhcpClientRenewSuccess
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

3.10.10 dhcpv4RelayAdminDisable

Table 181: 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

3.10.11 dhcpv4RelayAdminEnable

Table 182: 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
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

3.10.12 dhcpv4RelayAllDhcpv4ServersUnreachable

Table 183: 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

3.10.13 dhcpv4RelayOperDown

Table 184: 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

3.10.14 dhcpv4RelayOperUp

Table 185: 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

3.10.15 dhcpv6RelayAdminDisable

Table 186: dhcpv6RelayAdminDisable properties

Property name	Value
Application name	dhcp
Event name	dhcpv6RelayAdminDisable

Property name	Value
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

3.10.16 dhcpv6RelayAdminEnable

Table 187: dhcpv6RelayAdminEnable properties

Property name	Value
Application name	dhcp
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

3.10.17 dhcpv6RelayAllDhcpv6ServersUnreachable

Table 188: dhcpv6RelayAllDhcpv6ServersUnreachable properties

Property name	Value
Application name	dhcp
Event name	dhcpv6RelayAllDhcpv6ServersUnreachable
Default severity	critical

Property name	Value
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

3.10.18 dhcpv6RelayOperDown

Table 189: dhcpv6RelayOperDown properties

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

3.10.19 dhcpv6RelayOperUp

Table 190: 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

3.10.20 giAddressMismatch

Table 191: 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

3.10.21 sourceAddressMismatch

Table 192: 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

3.11 evpn

3.11.1 ethernetsegmentNetworkInstanceBgpInstanceDfStatusChanged

Table 193: 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.

3.11.2 ethernetsegmentPreferenceOperValueChanged

Table 194: 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.

3.11.3 evpnAutoDiscoveryEviRouteAddDroppedDueToUnexpectedEthTag

Table 195: 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

3.11.4 evpnAutoDiscoveryEviRouteWithdrawDroppedDueToUnexpectedEthTag

Table 196: 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

3.11.5 evpnAutoDiscoveryEviRouteWithdrawnDueToUnexpectedVni

Table 197: 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

3.11.6 evpnInclMcastRouteAddDroppedDueToUnexpectedEthTag

Table 198: 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

3.11.7 evpnInclMcastRouteWithdrawDroppedDueToUnexpectedEthTag

Table 199: 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

3.11.8 evpnInclMcastRouteWithdrawnDueToUnexpectedVni

Table 200: 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

3.11.9 evpnIpPrefixRouteNotImportedDueToUnexpectedVni

Table 201: 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

3.11.10 evpnIpPrefixRouteWithdrawnDueToNoGwMac

Table 202: 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

3.11.11 evpnIpPrefixRouteWithdrawnDueToUnexpectedGwIp

Table 203: 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

3.11.12 evpnMacRouteAddDroppedDueToUnexpectedEthTag

Table 204: 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

3.11.13 evpnMacRouteWithdrawDroppedDueToUnexpectedEthTag

Table 205: 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,

Property name	Value
	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 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

3.11.14 evpnMacRouteWithdrawnDueToUnexpectedVni

Table 206: 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

3.12 gnmi

3.12.1 globalConfigUpdate

Table 207: 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.

3.12.2 gnmiServerStart

Table 208: 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.

3.12.3 gnmiServerStop

Table 209: gnmiServerStop properties

Property name	Value
Application name	gnmi

Property name	Value
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.

3.12.4 networkInstanceConfigUpdate

Table 210: 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.

3.12.5 subscriptionEnd

Table 211: subscriptionEnd properties

Property name	Value
Application name	gnmi
Event name	subscriptionEnd
Default severity	informational

Property name	Value
Message format string	Subscription for path ' **path**' requested by **peer_address**:**socket** has finished.
Cause	A subscription has finished based on the request from mentioned peer.
Effect	none.

3.12.6 subscriptionRequestReceived

Table 212: 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.

3.12.7 subscriptionStart

Table 213: subscriptionStart properties

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

3.12.8 unixSocketGnmiOperDown

Table 214: 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.

3.12.9 unixSocketGnmiOperUp

Table 215: 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.

3.13 isis

3.13.1 isisAdjacencyBfdSessionSetupFailed

Table 216: 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.

3.13.2 isisAdjacencyChange

Table 217: 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.

3.13.3 isisAdjacencyRestartStatusChange

Table 218: 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

3.13.4 isisAreaMismatch

Table 219: 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

3.13.5 isisAuthDataFail

Table 220: 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

3.13.6 isisAuthTypeMismatch

Table 221: 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

3.13.7 isisCircuitIdsExhausted

Table 222: 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

3.13.8 isisCircuitMtuTooLow

Table 223: 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

3.13.9 isisCorruptedLspDetected

Table 224: 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

3.13.10 isisLdpSyncExited

Table 225: 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.

3.13.11 isisLdpSyncTimerStarted

Table 226: 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.

3.13.12 isisLspFragmentTooLarge

Table 227: 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

3.13.13 isisLspPurge

Table 228: 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**.

Property name	Value
Cause	LSP lifetime expired or other reason
Effect	The PDU is removed

3.13.14 isisLspSequenceNumberSkip

Table 229: 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

3.13.15 isisMaxAreaAddressesMismatch

Table 230: 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

3.13.16 isisMaxLspSequenceNumberExceeded

Table 231: 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

3.13.17 isisOverloadEntry

Table 232: 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.

3.13.18 isisOverloadExit

Table 233: 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.

3.13.19 isisOwnLspPurge

Table 234: 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

3.13.20 isisSystemIdLengthMismatch

Table 235: 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

3.13.21 isisVersionMismatch

Table 236: 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

3.14 json

3.14.1 authenticationError

Table 237: authenticationError properties

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

Property name	Value
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.

3.14.2 globalConfigUpdate

Table 238: 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.

3.14.3 httpJsonRpcOperDown

Table 239: 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.

Property name	Value
Effect	HTTP JSON RPC server on the mentioned network instance is now down.

3.14.4 httpJsonRpcOperUp

Table 240: 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.

3.14.5 httpsJsonRpcOperDown

Table 241: 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.

3.14.6 httpsJsonRpcOperUp

Table 242: 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.

3.14.7 jsonRpcRequestReceived

Table 243: 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.

3.14.8 jsonRpcResponseSent

Table 244: jsonRpcResponseSent properties

Property name	Value
Application name	json

Property name	Value
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.

3.14.9 networkInstanceConfigUpdate

Table 245: networkInstanceConfigUpdate properties

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

3.14.10 unixSocketJsonRpcOperDown

Table 246: 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.

Property name	Value
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.

3.14.11 unixSocketJsonRpcOperUp

Table 247: 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.

3.14.12 userAuthenticated

Table 248: 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.

3.14.13 userAuthenticationErrorWrongPassword

Table 249: 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.

3.15 lag

3.15.1 lagDown

Table 250: 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.

3.15.2 lagDownMinLinks

Table 251: 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.

3.15.3 lagMemberLinkAdded

Table 252: 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.

3.15.4 lagMemberLinkRemoved

Table 253: 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.

3.15.5 lagMemberOperDown

Table 254: lagMemberOperDown properties

Property name	Value
Application name	lag
Event name	lagMemberOperDown
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.

3.15.6 lagMemberOperUp

Table 255: lagMemberOperUp properties

Property name	Value
Application name	lag

Property name	Value
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.

3.15.7 lagUp

Table 256: 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.
Effect	The LAG is now operational.

3.16 ldp

3.16.1 ldpInterfaceDown

Table 257: ldpInterfaceDown properties

Property name	Value
Application name	ldp
Event name	ldpInterfaceDown
Default severity	warning

Property name	Value
Message format string	In network-instance **network_instance**, LDP has changed oper-state to DOWN on interface **subinterface**. The reason is **oper_down_reason**
Cause	This event is generated when LDP ceases to be functional on a subinterface.
Effect	LDP drops its adjacencies and sessions with other routers reachable through this subinterface.

3.16.2 ldpInterfaceUp

Table 258: ldpInterfaceUp properties

Property name	Value
Application name	ldp
Event name	ldpInterfaceUp
Default severity	notice
Message format string	In network-instance **network_instance**, LDP is now up and functional on interface **subinterface**.
Cause	This event is generated when LDP becomes functional on a suinterface.
Effect	LDP can form adjacencies and sessions with other routers reachable through this subinterface.

3.16.3 ldpIpv4InstanceDown

Table 259: ldpIpv4InstanceDown properties

Property name	Value
Application name	ldp
Event name	ldpIpv4InstanceDown
Default severity	warning
Message format string	In network-instance **network_instance**, LDP-IPv4 has changed oper-state to DOWN. The reason is **oper_down_reason**

Property name	Value
Cause	This event is generated when LDP ceases to becomes functional for IPv4 adjacencies, FECs and addresses.
Effect	LDP cannot form IPv4 adjacencies and sessions with other such routers.

3.16.4 ldpIpv4InstanceUp

Table 260: ldpIpv4InstanceUp properties

Property name	Value
Application name	ldp
Event name	ldpIpv4InstanceUp
Default severity	notice
Message format string	In network-instance **network_instance**, LDP-IPv4 is now up and functional.
Cause	This event is generated when LDP becomes functional for IPv4 adjacencies, FECs and addresses.
Effect	LDP can form IPv4 adjacencies and sessions with other such routers reachable through LDP interfaces that are operational.

3.16.5 ldpSessionDown

Table 261: ldpSessionDown properties

Property name	Value
Application name	ldp
Event name	ldpSessionDown
Default severity	warning
Message format string	In network-instance **network_instance**, the LDP session with peer **peer_ldp_id** has changed to non-existent.
Cause	This event is generated when an LDP session transitions into the non-existent state from a higher state.

Property name	Value
Effect	LDP immediately deletes FEC-label and address bindings received from this peer.

3.16.6 ldpSessionFecLimitReached

Table 262: ldpSessionFecLimitReached properties

Property name	Value
Application name	ldp
Event name	ldpSessionFecLimitReached
Default severity	warning
Message format string	The number of FECs received from the LDP peer **peer_ldp_id** has reached the configured limit of **fec_limit**.
Cause	The number of FECs accepted from the peer has reached the configured limit. If the number of FECs go below the limit and again start to increase and hit the limit a second time, a new event is generated if 2 or more minutes have elapsed since the previous event. If the FEC limit is changed and the current number of FECs is equal to or higher than the limit then the event is generated immediately.
Effect	If the peer supports the overload capability then the session will go into overload. If the peer doesn't support the overload capability then excess FECs will trigger the sending of label release messages back to the peer.

3.16.7 ldpSessionLocalIPv4Overload

Table 263: ldpSessionLocalIPv4Overload properties

Property name	Value
Application name	ldp
Event name	ldpSessionLocalIPv4Overload
Default severity	warning
Message format string	The LDP session with peer **peer_ldp_id** has entered overload for IPv4 FECs because this router sent an overload TLV to the peer.
Cause	The local router has received too many IPv4 FECs.

Property name	Value
Effect	The local router is requesting the peer to stop sending further IPv4 FECs.

3.16.8 ldpSessionPeerIPv4Overload

Table 264: ldpSessionPeerIPv4Overload properties

Property name	Value
Application name	ldp
Event name	ldpSessionPeerIPv4Overload
Default severity	warning
Message format string	The LDP session with peer **peer_ldp_id** has entered overload for IPv4 FECs because the peer sent an overload TLV.
Cause	The peer router has received too many IPv4 FECs.
Effect	The local router stops sending further IPv4 FECs to the peer.

3.16.9 ldpSessionUp

Table 265: ldpSessionUp properties

Property name	Value
Application name	ldp
Event name	ldpSessionUp
Default severity	notice
Message format string	In network-instance **network_instance**, an LDP session is now up and operational with peer **peer_ldp_id**.
Cause	This event is generated when an LDP session transitions into the operational state from a lower state.
Effect	LDP can exchange FEC-label and address bindings with this peer.

3.17 linux

3.17.1 cpuUsageCritical

Table 266: 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.

3.17.2 cpuUsageHigh

Table 267: 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.

3.17.3 cpuUsageNormal

Table 268: 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.

3.17.4 dateAndTimeChanged

Table 269: 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.

3.17.5 domainChanged

Table 270: domainChanged properties

Property name	Value
Application name	linux
Event name	domainChanged

Property name	Value
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.

3.17.6 hostnameChanged

Table 271: 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.

3.17.7 memoryUsageCritical

Table 272: 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.
Effect	No immediate effect, if utilization continues to increase, new memory allocations may fail, resulting in potential application failures.

3.17.8 memoryUsageFull

Table 273: 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.

3.17.9 memoryUsageHigh

Table 274: 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.

3.17.10 memoryUsageNormal

Table 275: 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.

3.17.11 partitionStateChange

Table 276: 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.

3.17.12 partitionUsageCritical

Table 277: 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.

3.17.13 partitionUsageFull

Table 278: 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.

3.17.14 partitionUsageNormal

Table 279: 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%.

Property name	Value
Effect	None.

3.17.15 partitionUsageWarning

Table 280: 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.

3.17.16 serviceConfigChanged

Table 281: 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.

3.17.17 serviceDownInNetworkInstance

Table 282: serviceDownInNetworkInstance properties

Property name	Value
Application name	linux
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.

3.17.18 serviceUpInNetworkInstance

Table 283: 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.

3.17.19 tlsProfileExpired

Table 284: tlsProfileExpired properties

Property name	Value
Application name	linux

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

3.17.20 tlsProfileExpiresSoon

Table 285: 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.

3.18 lldp

3.18.1 remotePeerAdded

Table 286: remotePeerAdded properties

Property name	Value
Application name	lldp
Event name	remotePeerAdded
Default severity	informational

Property name	Value
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.

3.18.2 remotePeerRemoved

Table 287: 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.

3.18.3 remotePeerUpdated

Table 288: 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**

Property name	Value
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.

3.19 log

3.19.1 bufferRollover

Table 289: 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.

3.19.2 configUpdate

Table 290: 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.

Property name	Value
Effect	Rsyslogd configuration has been modified, and the process has been restarted.

3.19.3 fileRollover

Table 291: 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.

3.19.4 networkNamespaceChanged

Table 292: 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.

3.19.5 subsystemFacilityChanged

Table 293: subsystemFacilityChanged properties

Property name	Value
Application name	log
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.

3.20 mgmt

3.20.1 checkpointGenerated

Table 294: 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.

3.20.2 checkpointRevertRequestReceived

Table 295: 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.

3.20.3 commitFailed

Table 296: 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

3.20.4 commitSucceeded

Table 297: commitSucceeded properties

Property name	Value
Application name	mgmt
Event name	commitSucceeded

Property name	Value
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

3.20.5 exclusiveConfigSessionBlockedByOtherSessionError

Table 298: exclusiveConfigSessionBlockedByOtherSessionError properties

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

3.20.6 exclusiveConfigSessionError

Table 299: 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**.

Property name	Value
Cause	Candidate datastore is locked due to other active session in progress
Effect	Exclusive configuration session Error

3.20.7 privateConfigSessionError

Table 300: 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
Effect	Private configuration session Error

3.20.8 privateSharedMismatch

Table 301: 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

3.20.9 sharedConfigSessionBlockedByOtherSessionError

Table 302: 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

3.21 netinst

3.21.1 networkInstanceInterfaceDown

Table 303: 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

3.21.2 networkInstanceInterfaceUp

Table 304: 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

3.21.3 networkInstanceStateDown

Table 305: 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

3.21.4 networkInstanceStateUp

Table 306: networkInstanceStateUp properties

Property name	Value
Application name	netinst
Event name	networkInstanceStateUp

Property name	Value
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

3.22 ospf

3.22.1 ospfAdjacencyBfdSessionSetupFailed

Table 307: 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.

3.22.2 ospfAdjacencyChange

Table 308: ospfAdjacencyChange properties

Property name	Value
Application name	ospf
Event name	ospfAdjacencyChange
Default severity	warning

Property name	Value
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.

3.22.3 ospfAdjacencyRestartStatusChange

Table 309: 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

3.22.4 ospfAsMaxAgeLSA

Table 310: 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**.

Property name	Value
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.

3.22.5 ospfExportLimitReached

Table 311: 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.

3.22.6 ospfExportLimitWarning

Table 312: 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.

3.22.7 ospfFailure

Table 313: 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.

3.22.8 ospfIfLdpSyncStateChange

Table 314: 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 **ospfIfLdpSync State**
Cause	This event is generated when an OSPF interface ldp-synchronization changes state.
Effect	Metric of the interface changes to or from infinity.

3.22.9 ospfIfRxBadPacket

Table 315: ospfIfRxBadPacket properties

Property name	Value
Application name	ospf

Property name	Value
Event name	ospfIfRxBadPacket
Default severity	warning
Message format string	Network-instance **network_instance** - OSPF instance **ospfInstance**: A bad packet was received on interface **subinterface** from **ospfPacket SrcAddress** 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

3.22.10 ospfIfStateChange

Table 316: 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.

3.22.11 ospfLsdbApproachingOverflow

Table 317: ospfLsdbApproachingOverflow properties

Property name	Value
Application name	ospf
Event name	ospfLsdbApproachingOverflow
Default severity	warning

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

3.22.12 ospfLsdbOverflow

Table 318: 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 **ospf ExtLsdbLimit**.
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.

3.22.13 ospfNbrMtuMismatch

Table 319: 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.

Property name	Value
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.

3.22.14 ospfOverloadEntry

Table 320: 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 **ospf OverloadReason**.
Cause	Overload bit configuration
Effect	No transit traffic is routed through the overloaded router.

3.22.15 ospfOverloadExit

Table 321: 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.

3.22.16 ospfOverloadWarning

Table 322: ospfOverloadWarning properties

Property name	Value
Application name	ospf
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.

3.22.17 ospfSpfRunRestarted

Table 323: 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.

3.22.18 ospfSpfRunsStopped

Table 324: ospfSpfRunsStopped properties

Property name	Value
Application name	ospf

Property name	Value
Event name	ospfSpfRunsStopped
Default severity	warning
Message format string	Network-instance **network_instance** - OSPF instance **ospfInstance**: SPF runs stopped - insufficient memory resources.
Cause	There are insufficient memory resources on the system to run the SPF to completion.
Effect	OSPF stops running SPFs until enough memory resources become available.

3.22.19 ospIfAuthDataFailure

Table 325: 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 **ospfPacketSrc Address** and packet type **ospfPacketType**, failed authentication with **ospfAuthError**
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

3.23 platform

3.23.1 airflowCorrected

Table 326: 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.

3.23.2 airflowMismatch

Table 327: 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.

3.23.3 componentBooting

Table 328: 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.

3.23.4 componentDown

Table 329: 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.

3.23.5 componentFailed

Table 330: 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.

3.23.6 componentInserted

Table 331: 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.

3.23.7 componentLocatorDisabled

Table 332: 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.

3.23.8 componentLocatorEnabled

Table 333: 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.

3.23.9 componentRemoved

Table 334: 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.

3.23.10 componentRestarted

Table 335: 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.

3.23.11 componentTemperatureExceeded

Table 336: 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.

3.23.12 componentTemperatureFailure

Table 337: componentTemperatureFailure properties

Property name	Value
Application name	platform

Property name	Value
Event name	componentTemperatureFailure
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.

3.23.13 componentTemperatureNormal

Table 338: 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.

3.23.14 componentUp

Table 339: componentUp properties

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

Property name	Value
Message format string	Component **type slot** is now operational
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.

3.23.15 controlModuleActivityChange

Table 340: 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.

3.23.16 controlModuleConfigSynchronized

Table 341: 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.

3.23.17 controlModuleImageSynchronized

Table 342: 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.

3.23.18 controlModuleInSync

Table 343: 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.

3.23.19 controlModuleOverlaySynchronized

Table 344: controlModuleOverlaySynchronized properties

Property name	Value
Application name	platform

Property name	Value
Event name	controlModuleOverlaySynchronized
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.

3.23.20 controlModuleSyncLost

Table 345: 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.

3.23.21 controlModuleSyncStart

Table 346: controlModuleSyncStart properties

Property name	Value
Application name	platform
Event name	controlModuleSyncStart
Default severity	informational

Property name	Value
Message format string	Active and standby control modules are now synchronizing **synchronization_category**
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.

3.23.22 fantrayEmpty

Table 347: 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.

3.23.23 linecardCapacityDegraded

Table 348: linecardCapacityDegraded properties

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

3.23.24 linecardCapacityNormal

Table 349: linecardCapacityNormal properties

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

3.23.25 platformLowPower

Table 350: 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.

3.23.26 platformLowReservePower

Table 351: platformLowReservePower properties

Property name	Value
Application name	platform

Property name	Value
Event name	platformLowReservePower
Default severity	critical
Message format string	Insufficient reserve power for currently installed components, **current_powerW** 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.

3.23.27 platformNormalPower

Table 352: platformNormalPower properties

Property name	Value
Application name	platform
Event name	platformNormalPower
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.

3.23.28 psuInputDown

Table 353: 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

Property name	Value
Cause	Input fault on the specified power supply is set.
Effect	The specified power supply can no longer supply power to the system.

3.23.29 psuInputUp

Table 354: 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.

3.23.30 psuOutputDown

Table 355: 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.

3.23.31 psuOutputUp

Table 356: psuOutputUp properties

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

3.23.32 psuTemperatureFault

Table 357: 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.

3.23.33 psuTemperatureNormal

Table 358: psuTemperatureNormal properties

Property name	Value
Application name	platform
Event name	psuTemperatureNormal

Property name	Value
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.

3.23.34 systemInServiceSoftwareUpgrade

Table 359: 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.

3.23.35 systemReboot

Table 360: systemReboot properties

Property name	Value
Application name	platform
Event name	systemReboot
Default severity	critical
Message format string	System going down for reboot

Property name	Value
Cause	The systemReboot event is generated when a software triggered reboot has been made.
Effect	The system will go offline for reboot.

3.23.36 systemWarmReboot

Table 361: 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.

3.23.37 systemWarmRebootAborted

Table 362: 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.

3.24 qos

3.24.1 platformQoSProfileHighUtilization

Table 363: 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

3.24.2 platformQoSProfileHighUtilizationLowered

Table 364: 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

3.25 ra_guard-agent

3.25.1 ra_guardAdd

Table 365: 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.

3.25.2 ra_guardRemove

Table 366: 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.

3.26 sflow

3.26.1 sFlowAgentChange

Table 367: 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.

3.26.2 sFlowCollectorUnreachable

Table 368: 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.

Customer document and product support

Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback