CHAPTER 16

Supported Service Alarms

These topics describe the service alarms supported by Cisco ANA:

- Service Alarms, page 16-2
- Registry Parameters, page 16-31

Each alarm is described in a section containing:

- A short description, including background about the network state or system (Cisco ANA) state that caused the alarm. The short description of the service alarm is what appears in the ticket, in the Service tab of Cisco ANA EventVision. The short description for each type and subtype can be viewed in Registry Parameters, page 16-31.

  When a flapping event occurs, the short description is changed.

Note The name of the service alarm is the same as the short description.

- A table of all the subtype events that represent one of the states the alarm can be in, and a description of when they are issued. For example, the Link Down alarm can have multiple subtype events (states) which include Link Down Due to Admin Down, Link Down Due to Oper Down, and Link Up. The description also shows if the event is a clearing event.
- Information related to the correlation of the alarm, mainly:
  - The alarm issue correlation process and location (local or network).
  - If other alarms can correlate to this alarm.
  - The keys that are used in the correlation process.
  - The specific correlation filters in use for the alarm, if any. The filter indicates if a specific event cannot be selected as the root cause event in the correlation process.
- By default, any new event filters the following events: Cloud Problem, BGP Process Down, LDP Neighbor Down, MPLS Interface Removed, the event itself, and events with lower or equal correlation weight.

Each section describes a group of alarms sharing the same event type.

Service Alarms

The following service alarms are supported in Cisco ANA:

Adaptive Polling

Adaptive polling is a mechanism that handles situations in which the device CPU is crossing a predefined, configurable threshold. It reduces the polling when the CPU reaches high threshold values for a configurable sample, and returns the polling to a normal rate when the CPU reaches the lower threshold. Where the CPU stays high for several samplings, the VNE is automatically moved to the maintenance state to avoid continuous polling of the device.

In all cases, alarms are issued when the device or the VNE state changes.

The source OID of this alarm is the Managed Element OID (IManagedElementOid), page 17-2.

Table 16-1 Adaptive Polling—Subtype Events

Subtype Event Name	Description
VNE Switched to Low Polling Rate Due to CPU High Usage	Issued when the CPU level has been above the high threshold (configurable, default=90%) for several samplings (configurable, default=5). The polling rate of the device is lowered by adding a delay between requests (default delay is 500 msec).
VNE Switched Back to Regular Polling Rate	Clearing event. Issued when the CPU level has been below the lower threshold (configurable, default=70%) for several samplings (configurable, default=2). The polling rate of the device is changed back to normal (no delay between requests).
VNE Switched to Maintenance Mode Due to CPU High Usage	Issued when the VNE polling rate is lower but the CPU stays high for several samplings (configurable, default=10). The VNE is automatically moved to the maintenance state, which means it stops polling the device. This state cannot be automatically cleared when the CPU usage decreases; the user must manually change the VNE state from the maintenance state to Start (as described in *Cisco Active Network Abstraction 3.6.6 Administrator Guide*).

Correlation

The alarm correlates to other alarms using the local correlation mechanism with the ManagedElement key. No other alarms can correlate to it.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

All IP Interfaces Down

The All IP Interfaces Down alarm is used when *all* IP interfaces configured on the same port are down, and implies that another fault has occurred in lower layers (such as the physical layer). In this case, one alarm is issued, and all IP interface status alarms are correlated to it.

Table 16-2 All IP Interfaces Down—Subtype Events

Subtype Event Name	Description
All IP Interfaces Down	Issued when all the IP interfaces configured above a physical interface change their state to down.
Active IP Interface Found	Clearing event. Issued when at least one of the IP interfaces changes its state to up.

Correlation

The alarm correlates to other alarms using the local correlation mechanism with the PortLayer1 key representing the physical layer. The PortLayer1 key is the port that all the IP interfaces were configured on.

Other alarms might correlate to this alarm using the physical port key, in particular the Interface Status Down alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

BGP Link Down

When a connection between two BGP peers is lost, no route information is exchanged between the two peers. This situation affects the network connectivity because route entries which are not refreshed start to be dropped from the routing table, causing packets to be dropped.

In this scenario, when a BGP neighbor has an adjacent peer (meaning that it is connected to another BGP neighbor with a discovered link), a BGP Link Down alarm is issued. When the adjacent peer is not managed, a BGP Neighbor Loss alarm is issued. A VNE identifies this situation based on changes in the BGP neighbor table of the device.

Due to the nature of this fault, it is possible that one of the devices may be unreachable. In this case, the respective VNE does not identify the changes in the BGP neighbor table of the unreachable device, but a BGP Link Down is still issued.

A negotiation process between the two link edges is issued when the BGP neighbor entry state changes from Established, indicating that a BGP Link Down should be invoked.

Table 16-3 BGP link down—Subtype Events

Subtype Event Name	Description
BGP Link Down	Issued when a BGP neighbor entry has changed its state from Established to another state, or a BGP neighbor entry that had an Established state has been removed from the BGP neighbors table and the entry has an adjacent peer. BGP neighbor state complies to the definitions in BGP4-MIB::bgpPeerState (1.3.6.1.2.1.15.3.1.2). In the case of a state change, any state other than Established implies the connection between the BGP peers is not fully functioning, meaning route information is not exchanged.
BGP Link Down VRF	Issued in the same conditions as the BGP Link Down alarm except that the neighbor is defined in the context of a VRF (BGP connection between PE router and CE router).
BGP Link Up	Clearing event. Issued when one of the edge BGP neighbor entries has changed its state from any state other than Established to Established. This is the clearing alarm for both the BGP Link Down alarms previously described.

Correlation

The alarm correlates to other alarms using the network correlation mechanism that runs a forward IP flow to the BGP neighbor peer IP. This flow runs a forward flow from each of the BGP neighbors to its peer IP, and might collect the following alarms: Interface Status Down, Port Down, Link Down, Device Unreachable, and so on.

Other alarms might correlate to it using the MPBgp key or the MPBgp key concatenated with the neighbor peer IP. Furthermore, the relevant BGP Neighbor Down syslogs are correlated to the service alarm.

Note The BGP Link Down and BGP Link Down VRF alarms do not filter out the BGP Process Down alarm in the correlation process.

Source OID

See MpBgp OID (IMpBgpOid), page 17-6.

BGP Neighbor Loss

A BGP Neighbor Loss alarm is issued when a BGP neighbor has an adjacent peer which is not managed.

When a connection between two BGP peers is lost, no route information is exchanged between the two peers. This situation affects the network connectivity because route entries which are not refreshed start to be dropped from the routing table after a while, causing packets to be dropped.

In this scenario, if only one of the peers is managed, a BGP Neighbor Loss alarm is issued instead of a BGP Link Down alarm. A VNE identifies this situation based on changes in the BGP neighbor table of the device.

Due to the nature of this fault, it is possible that one of the devices may be unreachable. In this case, the respective VNE cannot identify the changes in the BGP neighbor table of the unreachable device, and thus does not issue the alarm although the BGP connection has been lost. Only one alarm is issued from the reachable side.

Table 16-4 BGP Neighbor Loss—Subtype Events

Subtype Event Name	Description
BGP Neighbor Loss.	Issued when a BGP neighbor entry has changed its state from Established to another state, or when a BGP neighbor entry with the Established state has been removed from the BGP neighbors table. BGP neighbor state complies to the definitions in BGP4-MIB::bgpPeerState (1.3.6.1.2.1.15.3.1.2). In the case of a state change, any state other than Established implies that the connection between the BGP peers is not fully functioning, meaning that the route information is not exchanged.
BGP Neighbor Loss VRF	Issued in the same conditions as the BGP Neighbor Loss alarm, except that the neighbor is defined in the context of a VRF (BGP connection between PE router and CE router).
BGP Neighbor Found	Clearing event. Issued when a BGP neighbor entry has changed its state from any state other than Established to the Established state, or a new BGP neighbor entry that has an Established state has been discovered in the BGP neighbors table. This is the clearing alarm of both neighbor loss alarms previously described.

Correlation

The alarm correlates to other alarms using the network correlation mechanism that runs a forward IP flow to the BGP neighbor peer IP. This flow runs a forward flow from each of the BGP neighbors to its peer IP, and might collect the following alarms: Interface Status Down, Port Down, Link Down, Device Unreachable, and so on.

Other alarms might correlate to it using the MPBgp key or the MPBgp key concatenated with the neighbor peer IP. Furthermore, the relevant BGP Neighbor Down syslogs are correlated to the service alarm.

Note The BGP Neighbor Loss and BGP Neighbor Loss VRF alarms do not filter out the BGP Process Down alarm in the correlation process.

Impact Analysis

The alarm issues an impact analysis process that calculates the affected services of this fault. In this case, the affected service is represented as a pair of VRFs that cannot communicate due to this BGP Neighbor Loss fault.

The affected pair (service) can be marked as potentially affected or real affected. In this case, because the BGP reports on a neighbor loss only after a hold-time interval (default 180 sec), in which it did not get the hello message from its neighbor, it assumes that the connection was lost and cannot be recovered. The identified affected pairs are marked as real affected.

Source OID

See MpBgp OID (IMpBgpOid), page 17-6.

BGP Process Down

BGP Process Down is issued when the BGP process/service running on a device goes down. If such an alarm is not issued, a separate BGP Neighbor Loss alarm is created for each BGP neighbor, and these alarms are not correlated.

Table 16-5 BGP Process Down—Subtype Events

Subtype Event Name	Description
BGP Process Down	Issued when the BGP process/service is down after it was up. The BGP component in the VNE identifies this change, updates its state, and issues the alarm.
BGP Process Up	Clearing event. Issued when the BGP process/service changes its state back to up. The BGP component in the VNE identifies this change, updates its state, and issues the clearing alarm.

Correlation

Due to the nature of this alarm, it cannot be correlated to other alarms, thus this alarm does not try to run any correlation process.

Other alarms might correlate to it using the MPBgp key, in particular BGP Neighbor Loss alarms caused by this failure correlate to it.

Source OID

See MpBgp OID (IMpBgpOid), page 17-6.

Broken LSP Discovered

A Broken LSP Discovered alarm is issued as a companion to the MPLS Black Hole Found alarm (see MPLS Black Hole Found, page 16-68.)

An Broken LSP Discovered event means that an LSP, at some point, went through an MPLS black hole. Because of this the MPLS labels were removed from the packet, and one of the following scenarios occurs:

1. If the packet contains more than one MPLS label (data contained in the packet is VPN traffic), the packet is dropped or is forwarded to an incorrect destination. This happens because the IP header in the packet belongs to a different routing domain.
2. If the packet contains only one MPLS label (data contained in the packet belongs to the same routing domain), the packet continues to be forwarded based on the IP header information instead of the MPLS labels. This is not a problem.

The following information applies to the Broken LSP Discovered alarm:

- This alarm does not have a clearing alarm, which means that after it is issued, its severity cannot be changed.
- To overcome the previous limitation, the alarm auto-clear flag is set to true. This means that this alarm severity does not have an impact on the severity of other alarms that it correlates to.
- Though the Broken LSP Discovered alarm is issued as a companion to the MPLS Black Hole Found, it does not imply that it is issued from the same device that issued the MPLS Black Hole Found alarm.

After an MPLS Black Hole Found alarm is issued, a process starts and looks for broken LSPs that go through this MPLS black hole. The process of discovering the broken LSPs is as follows:

1. At the VNE on which the MPLS Black Hole Found was issued, all label switching entries that were destined for the black hole have an untagged out label. All MPLS labels are removed from packets traversing using this label switching entry.
2. Each untagged label switching entry starts traversing the LSP using a backward flow.

Note The direction of a backward flow traversing the VNE model is opposite that of a standard packet flow traversing the network.

3. On each device traversed in the backward flow,Cisco ANA checks for configured MPLS-based services on the device. Currently, the following identification services are supported:
   - Existence of VRFs (BGP/MPLS VPN services based on RFC2547).
   - Existence of MPLS Layer2 tunnels (PWE3 services based on RFC4448).
4. If the device contains such services, a Broken LSP Discovered alarm is issued for each LSP traversed backward to that point.

   This means that only PE routers issue such alarms. It is possible that the same LSP has entry points in multiple devices, and thus multiple alarms are issued for it.
5. Information that is important for each broken LSP alarm issued is the entry point (label switching entry) and the exit point (the IP subnet destination).

This information is used in the impact analysis process to identify the relevant affected pairs (services).

Table 16-6 Broken LSP Discovered—Subtype Events

Subtype Event Name	Description
Broken LSP Discovered	Issued as a companion to the MPLS Black Hole Found alarm as described previously. For every LSP traversing the black hole, a Broken LSP Discovered alarm is issued. There is no clearing event.

Correlation

This alarm is correlated by definition to one of the following:

- The MPLS Black Hole Found that triggered the discovery of this broken LSP.
- Link Down alarm, if the link down caused the MPLS traffic to change its course and pass through the black hole.

No other alarms can correlate to it.

Impact Analysis

The alarm issues an impact analysis process that identifies the local affected services of this fault. In this case, affected services can be of two types:

- A pair of VRFs that cannot communicate due to this broken LSP (for BGP/MPLS VPN services).
- A pair of MPLS Layer 2 tunnel edges representing a PWE3 service endpoint.

The affected pairs in this alarm are marked as potentially affected.

Note The system can be configured to present the affected pairs for BGP/MPLS VPN services as pairs of VRF IP interfaces instead of just the VRFs. This creates, in most cases, additional pairs that might cause a load on the system. Configuring them as IP interfaces is disabled by default.

Source OID

See LSE Entry OID (IMplsEntryOid), page 17-8 (the LSE entry that is the entry point to the broken LSP).

Card Down

The Card Down alarm represents a state in which a card is not operational. This can be caused by a hardware failure, or by changing the administrative state of the card.

Table 16-7 Card Down—Subtype Events

Subtype Event Name	Description
Card Down	Issued when the operational state of a card is changed to down. This can be caused by a hardware failure, or by changing the administrative state of the card
Card Up	Clearing event. Issued when the operational state of the card changes back to up.

Correlation

Due to the nature of this alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

Other alarms might correlate to it using the Card key.

Source OID

See Module OID (IModuleOid), page 17-5.

Card Out

The Card Out alarm represents a state where a card is removed from the device. The Card Out alarm is also issued when a device stops reporting on the existence of a card due to another failure, even if the card is actually still in the device. It is assumed that any functionality that was implemented by the card is not working anymore if the card had no redundancy configuration.

Note When a Card Out alarm occurs, Cisco ANA NetworkVision displays an alarm icon next to the affected card in the Inventory display. Even though the card has been physically removed, it is still displayed in Cisco ANA NetworkVision so that you can identify which network element is generating the alarm.

Table 16-8 Card Out—Subtype Events

Subtype Event Name	Description
Card Out	Issued when a card is removed from the device. It is possible that some card failures are identified as Card Out because the device does not report on the card’s existence after a failure.
Subcard Out	Issued when a card that is contained in another card is removed from the device. When a card that contains other cards is removed, in addition to the Card Out alarm issued on the main card, a Subcard Out alarm is issued for each of its subcards. It is possible that some failures of cards that contain subcards are identified as Card Down on the parent card and Subcard Out for the subcards, because the device stops reporting on the existence of the subcards.
Card In	Clearing event. Issued when the card is inserted back into the device.

Correlation

Due to the nature of the Card Out alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket. The Subcard Out alarm correlates to other alarms using the local correlation mechanism with Subcard key and its parent Card key.

Other alarms might correlate to it using the Card and Subcard keys.

Source OID

See Module OID (IModuleOid), page 17-5.

Cloud Problem

Cloud VNEs represent unmanaged network segments, so that operations such PathTracer and Root Cause Analysis (RCA) can be viewed or processed end-to-end. A Cloud VNE represents the unmanaged segment of a network as a single device to which two or more managed segments of the network can be connected.

In a network in which a segment of the network is unmanaged, Cisco ANA runs a correlation flow to find the root cause. If no root cause is found within the managed segment, a Cloud Problem service alarm is created, to which events are correlated.

Table 16-9 Cloud Problem—Subtype Events

Subtype Event Name	Description
Cloud Problem	An alarm might use network correlation using IP-based forward flow to a destination. During the flow, the alarm collects possible alarms with which to correlate. If it can not find no such alarms, and the flow has traversed a Cloud VNE (that is a network segment which is unmanaged by Cisco ANA), at the end of the flow a Cloud Problem alarm is issued. The original alarm is correlated to it. This alarm does not have a clearing alarm, thus the severity of the Cloud Problem alarm is informational

Correlation

Due to the nature of the Cloud Problem alarm, the event does not try to correlate to another event, but creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

Note When required, a correlation filter filters the Cloud Problem alarm. This enables or disables the ability of an alarm to create a Cloud Problem alarm and to correlate to it. The default value is false for all alarms in the system, meaning that an alarm does not correlate to the Cloud Problem alarm by default. However, there are several events that override the default configuration (these events are specific to Cisco devices) and are set to true, as follows:

- BGP Neighbor Down syslog
- OSPF Neighbor Loss syslog
- EIGRP Router Query to Neighbors Timeouted syslog

As described previously, other alarms might be correlated to it using the logic in the Cloud Problem subalarm. See Cloud Problem, page 16-10.

Note The Cloud Problem alarm does not filter the BGP Process Down alarm in the correlation process.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

Component Unreachable

A VNE might be configured to poll its respective device in multiple network protocols (for example both SNMP and Telnet). In addition, each protocol can be configured for reachability testing. This means that when the VNE stops responding using a protocol, the device is considered unreachable.

Table 16-10 Component Unreachable—Subtype Events

Subtype Event Name	Description
Device Unreachable	Issued when the device is not responding to at least one of the network protocols that are configured for reachability. The VNE uses a retry mechanism to make sure the problem persists for a certain configurable duration before issuing an alarm. This means that it is resilient during short periods of network packet loss. **Note** Cisco ANA will generate Device Unreachable events, with corresponding SNMP Timeout messages in the AVM log file, for devices with nonunique SNMP engine IDs. These IDs are normally derived from the device's unique MAC address and assigned automatically. They can also be user-customized. We recommend that you avoid custom SNMP engine IDs. If you do use them, make sure they are unique.
Device Reachable	Clearing event. Issued when the device responds to all the network protocols that are configured for reachability.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2 (the managed element of the Cloud VNE).

Checking Reachability

Reachability used by the VNEs (to check the reachability between the VNEs and network elements) depends on the configuration of the VNE, and involves multiple connectivity tests using SNMP, Telnet/SSH, and ICMP, as appropriate.

The following table describes the various situations where an NE fails to respond to the protocols:

Table 16-11 Unreachable Network Elements

VNE Type	Protocol Used to Check Reachability	Action Take When NE Fails to Respond	Action Taken When NE is Reachable
ICMP VNE	ICMP only. During the ICMP test, the unit pings the NE every configured interval.	ICMP ping is suspended, and a VNE Unreachable event is sent to the Cisco ANA Gateway. Thereafter, only the reachability tests are run to detect when the device is reachable again.	ICMP ping is restarted, and the alarm is cleared.
Generic VNE	• SNMP only (default). Polls the sysoid of the NE using an **SNMP get** command during the SNMP reachability test, and expects to receive a response; or • SNMP only (default), and adding an ICMP test.	General polling is suspended, and a VNE Unreachable event is sent to the Cisco ANA Gateway. Thereafter, only the reachability tests are run to detect when the device is reachable again. If more than one protocol is used, it is enough for one of them to become unreachable to generate the event. The event is generic to all the protocols.	• General polling is restarted, and all commands are sent to the device, smoothed across the polling interval. • The alarm is cleared.
Full VNE	• SNMP only (default). Polls the sysoid of the NE using an **SNMP get** command during the SNMP reachability test, and expects to receive a response; or • SNMP only (default), and adding ICMP and Telnet. During the Telnet test, the unit sends `Enter` via the open session and expects to get a prompt back.	General polling is suspended, and a VNE Unreachable event is sent to the Cisco ANA Gateway. Thereafter, only the reachability tests are run to detect when the device is reachable again. If more than one protocol is used, it is enough for one of them to become unreachable to generate the event. The event is generic to all the protocols.	• General polling is restarted, and all commands are sent to the device, smoothed across the polling interval. • The alarm is cleared.

Each of these scenarios has two possible settings in the registry:

- Track reachability (true/false). The default is true.

  When this parameter is true, reachability is tracked according to the specific protocol (ICMP, SNMP, Telnet, and so forth).

  When this parameter is false, the test is not performed.

- Lazy reachability (true/false). The default is false. This parameter determines whether there is a dedicated reachability command in charge of tracking reachability or whether reachability is determined by the regular polled commands.

  When this parameter is true, reachability is based on polling, and a dedicated command is not activated.

  When this parameter is false, a dedicated SNMP command is activated, and this test verifies the response from a specific SNMP OID (sysoid is the default that can be changed).

After the first failure of a command and all its retries, the device is considered unreachable. At this point, Cisco ANA starts to poll the device using the dedicated reachability command (see Table 16-11). In normal track reachability mode (lazy=false), the reachability commands run all the time. When the reachability test succeeds for the first time, it stops running and the device is considered reachable again.

Note Changes to the registry should be performed only with the support of Cisco. For details, contact your Cisco Account Team.

Correlation

The alarm correlates to other alarms using the network correlation mechanism, which runs a forward IP flow from the global routing entity to the management IP address (that is, to the IP address of the unit on which the VNE resides). This flow might collect the following alarms: Device Unreachable, Link Down, Port Down, Interface Status Down, BGP Neighbor Loss, and so forth.

Other alarms might correlate to it using the ManagedElement key.

Note The Device Unreachable alarm filters out the Link Down on Unreachable alarm in the correlation process. Events with the same weight are not filtered out.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

CPU Utilization

VNEs are configured to trace their device CPU utilization. An alarm is issued when device CPU utilization crosses a configured thresholds. The upper and lower thresholds are defined in the registry under the managed element.

Table 16-12 CPU utilization—Subtype Events

Subtype Event Name	Description
CPU Overutilized	Issued when the device CPU usage is above the configured upper threshold.
CPU Normal Utilization	Clearing event. Issued when the device CPU usage returns to below the lower threshold.

Correlation

Due to the nature of CPU utilization alarms, the event does not try to correlate to another event; it creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarm tries to correlate to this alarm.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

Device Unsupported

A VNE identifies various loading situations that prevent regular operation of the VNE. When such a situation occurs, the VNE issues a Device Unsupported alarm.

Table 16-13 Device unsupported—Subtype Events

Subtype Event Name	Description
Device Unsupported	Issued for the following scenarios: • The device type identified by its sysOid is not identified by the system. • The device software version is not supported, and the VNE is configured to react when a device is unsupported. Other possible actions are: use the default version, load generic VNE, or load ICMP VNE. • Registry problems occur when trying to load generic or ICMP VNEs. • The VNE failed to retrieve the device sysOid or software version.

Correlation

Due to the nature of the Device Unsupported alarm, the event does not try to correlate to another event and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

Dropped Packets

VNEs are configured to trace the dropped packet counters on their device ports. An alarm is issued when a dropped packet counter from a port crosses the configured thresholds. The upper and lower thresholds are defined in the registry under PortLayer1.

Table 16-14 Dropped packets—Subtype Events

Subtype Event Name	Description
Dropped Packets on Port	Issued when the number of dropped packets on a device port is higher than the configured threshold.
Stopped Dropping Packets on Port	Clearing event. Issued when the number dropped packets on a device port is lower than the configured threshold.

Correlation

Due to the nature of the Dropped Packets on Port alarm, the event does not try to correlate to another event and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

By default, impact analysis is not supported for this alarm, but it can be enabled. If enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, Port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

Discard Packets

VNEs are configured to trace the discarded packet counters on their device ports. An alarm is issued when the discarded counter for a port crosses the configured thresholds. The upper and lower thresholds are defined in the registry under the PortLayer1.

Table 16-15 Discard packets—Subtype Events

Subtype Event Name	Description
Discard Packets	Issued when the number of discarded packets on a device port is higher than the configured threshold.
Normal Discard Packets	Clearing alarm. Issued when the number of discarded packets on a devices port is lower than the configured threshold.

Correlation

Due to the nature of the Discard Packets alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

By default, impact analysis is not supported for this alarm, but it can be enabled. If enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, Port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

GRE Tunnel Down

Generic routing encapsulation (GRE) tunnels are basically stateless, meaning that when the tunnel is down, the tunnel edges might not identify this situation and continue reporting the tunnel as up. To overcome this, the GRE tunnel edge can be configured to send *keepalive* messages. If at some point a GRE tunnel edge does not receive keepalive messages, it can change its state to down.

The GRE Tunnel Down alarm is supported only on GRE tunnels that are configured with keepalive messages. When keepalive is configured on the GRE tunnel edge, if a failure occurs in the GRE tunnel at any point, both IP interfaces of the GRE tunnel edges change their state to down. This ensures that the alarm is identified. If keepalive is not configured on the GRE tunnel edge, because the alarm creation is triggered by the state change of the IP interface of the GRE tunnel, the GRE Tunnel Down alarm might not be generated.

Table 16-16 GRE Tunnel Down—Subtype Events

Subtype Event Name	Description
GRE Tunnel Down	Issued when a GRE link exists between the two tunnel edges and the state of the IP interface of one of the GRE tunnel edges changes to down. A simple negotiation procedure is done to avoid sending the event from both edges of the GRE tunnel, and a GRE Tunnel Down event is issued.
GRE Tunnel Up	Clearing event. Issued when the IP interface state changes back to up. The clearing event is issued even if the GRE link does not exist (for example, if the user has executed `clear&remove` on the event).

Correlation

The GRE Tunnel Down alarm tries to correlate to other alarms using the network correlation mechanism that runs a forward IP flow from the local GRE tunnel edge to the tunnel destination IP. This flow might collect the following alarms: Link Down, Port Down, Interface Status Down, and more.

Other alarms might correlate to it using the TunnelGre key.

Source OID

See Topological Link OID (ITopologicalLinkOid), page 17-2 (each endpoint is Layer 2 GRE Tunnel OID (ITunnelGreOid).

HSRP Group Status Changed

Hot Standby Router Protocol (HSRP) is used in IP networks and allows one router to automatically assume the function of the second router if the second router fails. The current support relates to the instance where only one backup router is configured in the HSRP group, though it is possible to configure more than one.

Table 16-17 HSRP group status changed—Subtype Events

Subtype Event Name	Description
Primary HSRP Interface Is Not Active	Issued when the primary interface within an HSRP group has changed its state to down. This means that one of the other interfaces in the group becomes the active interface in the group. This alarm tries to correlate to other alarms using the network correlation mechanism that runs a forward IP flow from the local global routing entity to the HSRP group backup interface IP. Alarms can correlate to this alarm using the local IPInterface key.
Primary HSRP Interface Is Active	Clearing event for the Primary HSRP Interface Is Not Active alarm. Issued when the primary interface within a HSRP group has changed its state back to up after it was down. This means that if one of the other interfaces in the group was currently active it becomes secondary. This alarm is the clearing alarm for the Primary HSRP Interface Is Not Active alarm.

Table 16-17 HSRP group status changed—Subtype Events (continued)

Subtype Event Name	Description
Secondary HSRP Interface Is Active	Issued when a secondary interface within an HSRP group has changed its state to up. This happens when the original active interface changes its state to down and the backup interface takes over. This alarm tries to correlate to other alarms using the network correlation mechanism that runs a forward IP flow from the local global routing entity to the HSRP group virtual IP. Alarms can correlate to this alarm using the local IPInterface key.
Secondary HSRP Interface Is Not Active	Clearing event for the Secondary HSRP Interface Is Active alarm. Issued when a secondary interface within a HSRP group has changed its state back to down after it was up. This means that the original active interface in that group has changed its state to up.

Correlation

For correlation to work, there must be a correlation path between the routers. Correlation details are described in the relevant subtype events in Table 16-17.

Source OID

See IP Interface OID (IPInterfaceOid), page 17-6 (IP interface of the active or secondary interface).

Interface Status

VNEs are configured to trace the operational state of their IP interfaces. When the status of an IP interface changes, the VNE issues the relevant alarm. There are multiple subtype events for Interface Status Down, and the subtype that is issued depends on the scenario. Each has a different behavior; these are described in Table 16-18.

Table 16-18 Interface status—Subtype Events

Subtype Event Name	Description
Interface Status Down (GRE tunnel)	Issued when the IP interface on a GRE tunnel changes its state to down. Correlation—This alarm issues a local correlation process and tries to correlate to the GRE Tunnel Down alarm. If the GRE tunnel down does not exist (for example, in the case where no GRE link exists), the alarm is issued as the root cause. When the GRE tunnel is issued from the other edge of the tunnel, it uses the local alarm to correlate to it. Other alarms might correlate to it using the IPInterface key. This includes alarms such as Device Unreachable or any other alarms that perform network correlation and where the correlation flow traverses the IP interface.
Interface Status Down (connection that is a point-to-point connection)	Issued when a point-to-point IP interface changes its state to down. The identification of this type of interface is done using the following: **1.** The subnet mask is /30 or /31. **2.** The IP interface is on one VC encapsulation. Correlation—The alarm correlates to other alarms using the network correlation mechanism that runs a forward down IP flow from the IP interface to other IP addresses in the IP interface's IP address subnet. This flow might collect the following alarms: Link Down, Port Down, and so on. Other alarms might correlate to it using the IPInterface or the physical port (PortLayer1) keys.
Interface Status Down (nonconnection that is a multipoint connection)	Issued when a point-to-point IP interface changes its state to down. The identification of this type of interface is done using the following: **1.** The number of encapsulations under the IP interface/MPLS is greater than one. **2.** Any other case not covered in the previously-described scenarios. Correlation—The alarm correlates to other alarms using the network correlation mechanism that runs a forward down flow from the IP interface to the Physical port (PortLayer1) under this interface.
Interface Status Up	Clearing event. Issued when an IP interface changes its operational state from down to up.

Correlation

Correlation details are described in the relevant subtype events in Table 16-18.

Source OID

See IP Interface OID (IPInterfaceOid), page 17-6.

Investigation State

Situations might occur where one or more physical components (specifically modules) are not identified by the physical investigation component in a VNE. This is not an unusual scenario because many devices have large sets of supported modules, and not all of the modules may be supported by the VNE. The Investigation State alarm is issued in this scenario.

Table 16-19 Investigation state—Subtype Events

Subtype Event Name	Description
Investigation State	Issued when one or more modules are not identified by the physical investigation component of the VNE. There is no clearing event.

Correlation

Due to the nature of the Investigation State alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

L2TP Peer Not Established

This alarm is specific to the Redback Networks implementation of Layer 2 Tunneling Protocol (L2TP), and is based on the state of an L2TP peer that is basically a logical entity from which L2TP tunnels are created. The L2TP peer is also used as a container for these L2TP tunnels. The alarm is issued when the L2TP peer has an incorrect tunnel configuration and the tunnels between the L2TP access concentrator (LAC) and the L2TP network server (LNS) cannot be created.

Table 16-20 L2TP Peer Not Established—Subtype Events

Subtype Event Name	Description
l2TP Peer Not Established	Issued when the L2TP peer has an incorrect configuration, and L2TP tunnels cannot be created between the LAC and the LNS. This is identified by querying the state of the L2TP peer tunnels that do not change to Established.
l2TP Peer Is Removed	Issued when the L2TP peer is removed from the L2TP peer list, or when the first tunnel in the peer changes its state from Established to another state.
l2TP Peer Established	Clearing event. Issued when at least one tunnel of the L2TP peer is in an Established state.

Correlation

The alarm correlates to other alarms using the network correlation mechanism that runs a forward down flow from the L2TP peer to the remote IP.

Other alarms can correlate to this alarm using the local L2TPpeer key.

Source OID

See L2TP Peer OID (IL2tpPeerOid), page 17-9.

L2TP Sessions Threshold

This alarm is specific to the Redback Networks implementation of L2TP and is implemented as a TCA of the number of sessions in a L2TP peer. The alarm is issued when the number of L2TP sessions related to the L2TP peer crosses a configurable threshold.

Table 16-21 L2tp sessions threshold—Subtype Events

Subtype Event Name	Description
l2TP Sessions Count Exceeds Maximum Threshold	Issued when the number of active sessions associated with the L2TP peer crosses a configurable threshold (the default is 80%). The calculation is done as follows: *active-sessions*/(*max-session-per-tunnel* * *max-tunnels-per-peer*) * 100.
l2TP Sessions Count Has Returned To Normal	Clearing event. Issued when the number of active sessions associated with the L2TP peer drops below the lower threshold (the default is 70%).

Correlation

Due to the nature of the L2TP Sessions Count Exceeds Maximum Threshold alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Source OID

See L2TP Peer OID (IL2tpPeerOid), page 17-9.

Note This alarm is implemented as TCA, which means that no information about this alarm is found in the standard event-related registry.

Layer 2 Tunnel Down

A Layer 2 tunnel represents a point-to-point pseudowire in the network, also known as an AToM. This alarm is issued when the operational state of a Layer 2 tunnel changes.

Table 16-22 Layer 2 tunnel down—Subtype Events

Subtype Event Name	Description
Layer 2 Tunnel Down	Issued when the operational state of the Layer 2 tunnel changes its state to down. This can happen due to a problem between the two edges of the tunnel or on the local tunnel interface. When the state changes on both edges, a simple negotiation procedure is done to avoid sending the alarm from both edges of the Layer 2 tunnel.
Layer 2 Tunnel Up	Clearing event. Issued when the Layer 2 tunnel changes its state back to up.

Correlation

Because this alarm can be caused by multiple conditions, it issues multiple network correlation flows, which run as follows:

- A network flow from the Layer 2 tunnel to the remote IP to identify problems that occur between the tunnel edges.

  This flow might collect the following alarms: Link Down, Port Down, MPLS alarms, and so on.
- A network flow from the local Layer 2 tunnel edge to the physical port on which it is configured, to identify problems that occur on the local physical interface.

  This flow might collect the following alarms: Link Down, Port Down, and so on.
- A network flow from the remote Layer 2 tunnel edge to the physical port on which it is configured, to identify problems that occur on the remote physical interface.

  This flow might collect the following alarms: Link Down, Port Down, and so on.

Any alarm can correlate to this alarm using the PTPLayer2MplsTunnel (which represents the Layer 2 tunnel edge) key.

Note The Layer 2 Tunnel Down alarm does not filter out the LDP Neighbor Down alarm in the correlation process.

Source OID

See Topological Link OID (ITopologicalLinkOid), page 17-2 (each endpoint is Layer 2 Mpls Tunnel OID (IPTPMplsLayer2TunnelOid).

LDP Neighbor Loss

VNEs are configured to trace the state of the current LDP neighbor of their devices. The VNE issues the relevant alarm when it identifies that an existing LDP neighbor has been removed, or that an LDP neighbor that was removed has been restored.

The identification of this alarm is expedited by notifications such as syslogs or traps.

Table 16-23 LDP neighbor loss—Subtype Events

Subtype Event Name	Description
LDP Neighbor Down	Issued when an LDP neighbor of the device that was previously discovered is removed.
LDP Neighbor Up	Clearing event. Issued when the LDP neighbor that was previously removed is restored and is currently active.

Correlation

This alarm issues a network correlation flow that runs a forward down flow from the global routing entity to the LDP peer IP address.

This flow might collect the following alarms: MPLS Interface Removed, Link Down, Port Down, and so on.

Any alarm can correlate to this alarm using the LDPPeer or LDPpeerDiscoverySources keys.

Note The LDP Neighbor Down alarm does not filter out the MPLS Interface Removed alarm in the correlation process.

Source OID

See LSE OID (ILseOid), page 17-7 (Label Switching Entity with the differentiator object of the LDP peer).

Link Down

This is one of the basic service alarms supported in the system. When a port has an adjacent peer (that is, it is connected to another port and has a discovered link), and its operational state changes from up to down or from down to up, the alarm is issued. When the port is not adjacent, a Port Down alarm is issued instead of a Link Down alarm. See Port Down, page 16-27.

The negotiation process between the two link edges occurs when the port's operational state changes to down to identify the exact event that should be issued.

Table 16-24 Link Down—Subtype Events

Subtype Event Name	Description
Link Down Due To Admin Down	Issued when the admin state of at least one of the link ports changes to down. Correlation—Due to the nature of this alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway that is the root cause alarm of the ticket.
Link Down Due To Oper Down	Issued when the admin state is up on both ports and none of the scenarios described below occur. Correlation—This alarm issues a local correlation process and tries to correlate to other alarms using the physical port (PortLayer1) key.
Link Down Due To Card Event	Issued when at least one of the ports is on a card that was removed from the device, or is currently in an operational down state. Correlation—This alarm issues a local correlation process and tries to correlate to other alarms (specifically Card Out or Card Down) using the Module key.
Link Down On Unreachable	Issued when at least one of the ports is on a device that is currently unreachable by its VNE. Correlation—This alarm issues a local correlation process in order to correlate to the Device Unreachable alarm (using the ManagedElement key).
Link Up	Clearing event. Issued when the port operational state changes back to up.

Link Down supports flapping with the following subevents:

- Link Down Flapping
- Link Down Flapping Update
- Link Down Stopped Flapping Cleared
- Link Down Stopped Flapping Noncleared

Note In Cisco ANA EventVision, these flapping subevent names are displayed in the event's short description field.

Correlation

Other alarms can try to correlate to any link down alarm using the Physical port (PortLayer1) key.

Source OID

Topological Link OID (ITopologicalLinkOid), page 17-2 (where each endpoint is Physical Layer OID (IPhysicalLayerOid), page 17-4).

Link Utilization

VNEs are configured to trace the Rx and Tx counters on their device ports, where a port has an adjacent peer (that is, it is connected to another port), and it already issued a Rx Overutilized or Tx Overutilized alarm. (For more information on these alarms, see Rx Utilization, page 16-29 and Tx Utilization, page 16-31.) This alarm has complementary functionality so that all the utilization alarms from both ports of the link correlate to it, instead of issuing multiple root cause alarms.

Table 16-25 Link utilization—Subtype Events

Subtype Event Name	Description
Link Overutilized	Issued after Tx Overutilized or Rx Overutilized alarms are issued on a physical port, if the port has an adjacent peer to enable correlation of all port level utilizations alarms from the ports on both sides of the link to one link utilization alarm.
Link Utilization Normal	Clearing event. Issued if both sides of the link send clearing alarms on the Tx utilization and Rx utilization alarms.

Correlation

Due to the nature of this alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

Other alarms can correlate to this alarm using the physical port (PortLayer1) key.

Source OID

Topological Link OID (ITopologicalLinkOid), page 17-2 (where each endpoint is Physical Layer OID (IPhysicalLayerOid), page 17-4).

Logical Port Down

Logical ports are logical interfaces that are defined on physical ports. Logical ports are used to logically separate the traffic of the physical port, and to control the separated traffic in a different manner. Logical ports are currently implemented in Cisco ANA for specific VNE types (for example, Lucent WAN Switches) and specific technologies (such as ATM and Frame Relay). Each logical port has an independent administrative and operational state. When the operational state of a logical port changes, the VNE issues an alarm.

Table 16-26 Logical port down—Subtype Events

Subtype Event Name	Description
Logical Port Down	Issued when the operational state of a logical port changes to down.
Logical Port Up	Clearing event. Issued when the operational state of a logical port changes back to up.

Correlation

This alarm issues a local correlation process and tries to correlate to alarms on the physical port using the physical port (PortLayer1) key. Possible alarms that this alarm can correlate to are Link Down, Port Down, or any alarm on the physical port.

Other alarms might correlate to it using the Logical port key, including alarms that perform network correlation, and the correlation flow traverses the logical port.

Note The Logical Port Down alarm does not filter out the BGP Process Down alarm in the correlation process.

Source OID

See Logical Port OID (ILogicalPortOid), page 17-9.

Memory Utilization

VNEs are configured to trace their device memory utilization. A memory utilization alarm is issued when the device memory utilization crosses a configured threshold. The upper and lower thresholds are defined in the registry under ManagedElement.

Table 16-27 Memory utilization—Subtype Events

Subtype Event Name	Description
Memory Overutilized	Issued when the device memory usage is above the configured upper threshold.
Memory OK	Clearing event. Issued when the device memory usage is back below the lower threshold.

Correlation

Due to the nature of the Memory Utilization alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Source OID

See Managed Element OID (IManagedElementOid), page 17-2.

MPLS Black Hole Found

A MPLS black hole is an abnormal termination of an MPLS path (an LSP) inside an MPLS network. A MPLS black hole exists when there are untagged entries destined for a known PE router on a specific interface. Note that the untagged interfaces might exist in the network in normal situations. For example, where the boundary of the MPLS cloud has untagged interfaces, this is still considered normal.

MPLS black hole cause the loss of all the MPLS labels on a packet, including the VPN information that lies in the inner MPLS label. Therefore, if a packet goes through an untagged interface, the VPN information is lost. The VPN information loss translates directly to VPN sites losing connectivity.

Black hole alarms are detected in either of the following situations:

- When the system is loaded for the first time and performs the initial discovery of the network.
- Changes in the network are identified through the ongoing discovery process.

Table 16-28 MPLS Black Hole Found found—Subtype Events

Subtype Event Name	Description
MPLS Black Hole Found	Issued when an MPLS interface has at least one untagged LSP leading to a known PE router; in other words, an LSE entry changed to an Untagged action with a PE as a next hop. After an MPLS Black Hole Found alarm is issued, a process begins looking for broken LSPs that go through the MPLS black hole. See Broken LSP Discovered, page 16-7.
MPLS Black Hole Cleared	Clearing event. Issued when the MPLS interface that had untagged LSPs to a known PE router has no more untagged entries to any known PE neighbor.

Correlation

The MPLS Black Hole Found alarm can correlate to MPLS Interface Removed and LDP Neighbor Loss alarms. Broken LSP Discovered alarms can correlate to MPLS Black Hole Found alarms.

Note The MPLS Black Hole Found alarm does not filter out the MPLS Interface Removed and LDP Neighbor Down alarms in the correlation process.

Source OID

See LSE OID (ILseOid), page 17-7 (appended with a differentiator of the next hop interface name).

MPLS Interface Removed

The MPLS interface is basically a representation of the MPLS sublayer in an interface configuration. The interface can be configured with or without MPLS capabilities. If this type of configuration change takes place while the VNE is loaded, it issues MPLS interface removed or added alarms.

Table 16-29 MPLS interface removed—Subtype Events

Subtype Event Name	Description
MPLS Interface Removed	Issued when an MPLS interface has at least one untagged LSP leading to a known PE router (that is, an LSE entry changed to an Untagged action with a PE as a next hop). After an MPLS Black Hole Found alarm is issued, a process that looks for broken LSPs that go through this MPLS black hole is started. See Broken LSP Discovered, page 16-7.
MPLS Interface Added	Clearing event. Issued when the MPLS capabilities of an interface are enabled after they were disabled.

Correlation

The alarm correlates to other alarms using the network correlation mechanism which runs a forward flow to the underlying physical port. This flow might collect the Card Out and Card Down alarms, because the only other cases in which it happens are due to other faults that are hardware related.

Other alarms might correlate to it using the MPLS key, including MPLS black hole alarms, MPLS TE Tunnel Down alarm, and so on.

Source OID

See LSE OID (ILseOid), page 17-7 (Label Switching Entity with differentiator object of the MPLS interface description).

MPLS-TE Tunnel Down

VNEs are configured to trace the operational state of their MPLS TE tunnel interfaces. When the state of the tunnel changes, the VNE issues the relevant alarm.

Table 16-30 MPLS TE Tunnel Down—Subtype Events

Subtype Event Name	Description
MPLS-TE tunnel Down	Issued when the tunnel changes it state to down. MPLS-TE Tunnel Down alarm supports flapping with the following subevents: • MPLS-TE Tunnel Flapping • MPLS-TE Tunnel Update • MPLS-TE Tunnel Stopped Flapping Cleared • MPLS-TE Tunnel Stopped Flapping Noncleared **Note** In Cisco ANA EventVision, these flapping subevent names are displayed in the event's short description field.
MPLS-TE Tunnel Up	Clearing event. Issued when an MPLS TE tunnel changes its operational state from down to up.

Correlation

For all the down alarms, any other alarm can try to correlate to this alarm using the MPLS TE tunnel OID (IMplsTETunnelOid) key. The alarm correlates to other alarms using the network correlation mechanism that runs a forward down IP flow from the MPLS TE tunnel to its tunnel destination IP address. This flow might collect the following alarms: Link Down, Port Down, and so on.

The MPLS-TE Tunnel Down alarm does not filter out the BGP Process Down alarm in the correlation process.

Source OID

See MPLS TE Tunnel OID (IMplsTETunnelOid), page 17-8.

Port Down

When a physical port does not have an adjacent peer (that is, it is connected to another port) and its operational state changes from up to down, or from down to up, port down alarms are issued. When the port does have an adjacent peer, instead of a Port Down alarm, a similar Link Down alarm is issued. See Link Down, page 16-22.

Table 16-31 Port Down—Subtype Events

Subtype Event Name	Description
Port Down	Issued when the operational state of a physical port changes to down. Port Down supports flapping with the following subevents: • Port Down Flapping • Port Down Flapping Update • Port Down Stopped Flapping Cleared • Port Down Stopped Flapping Noncleared.
Port Down Due To Card Event	Issued when the port is on a card that was removed from the device or is currently in an operational down state. Correlation—This alarm issues a local correlation process and tries to correlate to other alarms (specifically Card Out or Card Down) using the Module key.
Port Up	Clearing event. Issued when the operational state of a logical port changes back to up.

Correlation

For all the down alarms, any other alarm can try to correlate to this alarm using the Physical port (PortLayer1) key.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

Rx Dormant

VNEs are configured to trace the Rx packet counters on their device ports. An alarm is issued when the Rx counter on a port drops below the configured threshold.

Note This alarm is disabled by default.

Table 16-32 Port Down—Subtype Events

Subtype Event Name	Description
Rx Dormant	Issued when the number of Rx packets on a device port is lower than the configured threshold.
Rx Dormant Normal	Clearing event. Issued when the number of Rx packets on a device port returns to a number lower than the configured threshold.

Correlation

The port Rx Dormant alarm does not start a correlation process and is always issued as a root cause alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

Rx Utilization

VNEs are configured to trace the Rx packet counters on their device ports. An alarm is issued when a the Rx counter for a port crosses the configured thresholds. The upper and lower thresholds are defined in the registry under the PortLayer1. Where the port has an adjacent peer (that is, it is connected to another port) a Link Utilization alarm is also issued. For more information on these alarms, see Link Utilization, page 16-23.

Table 16-33 Rx utilization—Subtype Events

Subtype Event Name	Description
Rx Overutilized	Issued when the number of Rx packets on a device s port is higher than the configured threshold.
Rx Utilization Normal	Clearing event. Issued when the number of Rx packets on a device port returns to a number lower than the configured threshold.

Correlation

The Rx utilization alarms do not start a correlation process. No other alarms can correlate to this alarm, because there are no supported alarms that can be affected by the Rx utilization alarm.

Impact Analysis

Impact analysis is not supported by default for this alarm, but can be enabled. If it is enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

Shelf Out

The Shelf Out alarm represents a state in which the shelf is removed from the device. The Shelf Out alarm is also issued when the device stops reporting on the existence of a shelf due to another failure, even if the shelf is actually still in the device. It is assumed that any functionality that was implemented by the shelf is not working anymore if the shelf had no redundancy configuration.

Table 16-34 Shelf out—Subtype Events

Subtype Event Name	Description
Shelf Out	Issued when a shelf is removed from the device. It is possible that some shelf failures are identified as Shelf Out, because the device does not report on the shelf's existence after the failure.
Shelf In	Clearing event. Issued when the shelf is inserted back into the device.

Correlation

Due to the nature of the Shelf Out alarm, it does not start a correlation process and is always issued as a root cause alarm.

Other alarms might correlate to it using the Shelf key, such as the Card Out alarm.

Source OID

See Shelf OID (IShelfOid), page 17-5.

Tx Dormant

VNEs are configured to trace the Tx packet counters on their device ports. An alarm is issued when an Rx counter on a port drops below the configured thresholds. The upper and lower thresholds are defined in the registry under the PortLayer1.

Note This alarm is disabled by default.

Table 16-35 Shelf out—Subtype Events

Subtype Event Name	Description
Tx Dormant	Issued when the number of Tx packets on a device port is lower than the configured threshold.
Tx Dormant Normal	Clearing event. Issued when the number of Tx packets on a device port returns to a number higher than the configured threshold.

Correlation

The port Tx Dormant alarm does not start a correlation process and is always issued as a root cause alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

Tx Utilization

VNEs are configured to trace the Tx packets counters on their device ports. An alarm is issued when a Rx counter on a port crosses the configured thresholds. The upper and lower thresholds are defined in the registry under the PortLayer1. Where the port has an adjacent peer (that is, it is connected to another port), a Link Utilization alarm is also issued. For more information on these alarms, see Link Utilization, page 16-23.

Table 16-36 Shelf out—Subtype Events

Subtype Event Name	Description
Tx Overutilized	Issued when the number of Tx packets on a device port is higher than the configured threshold.
Tx Utilization Normal	Clearing event. Issued when the number of Tx packets on a device port returns to a number lower than the configured threshold.

Correlation

The port Tx Utilization alarm does not start a correlation process. No other alarm tries to correlate to this alarm, because there are no supported alarms that can be affected by the Tx Utilization on Port alarm.

Impact Analysis

Impact analysis is not supported by default for this alarm, but can be enabled. If impact analysis is enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid), page 17-4.

Registry Parameters

The following registry parameters are included in this section:

- Adaptive Polling, page 16-32
- All IP Interfaces Down, page 16-34
- BGP Link Down, page 16-35
- BGP Neighbor Loss, page 16-37
- BGP Process Down, page 16-39
- Broken LSP Discovered, page 16-40
- Card Down, page 16-41
- Card Out, page 16-42
- Cloud Problem, page 16-43
- Component Unreachable, page 16-44
- CPU Utilization, page 16-45

- Device Unsupported, page 16-46
- Dropped Packets, page 16-47
- Discard Packets, page 16-48
- GRE Tunnel Down, page 16-49
- HSRP Group Status Changed, page 16-50
- Interface Status, page 16-52
- Investigation State, page 16-55
- L2TP Peer Not Established, page 16-56
- L2tp Sessions Threshold, page 16-58
- Layer 2 Tunnel Down, page 16-59
- LDP Neighbor Loss, page 16-60
- Link Down, page 16-61
- Link Utilization, page 16-65
- Logical Port Down, page 16-66
- Memory Utilization, page 16-67
- MPLS Black Hole Found, page 16-68
- MPLS Interface Removed, page 16-69
- MPLS TE Tunnel Down, page 16-70
- Port Down, page 16-71
- Rx Dormant, page 16-74
- Rx Utilization, page 16-75
- Shelf Out, page 16-76
- Tx Dormant, page 16-77
- Tx Utilization, page 16-78

Adaptive Polling

Table 16-37 VNE Switched to Low Polling Rate Due to CPU High Usage

Service Alarm Setting	Registry Parameter
Type	Adaptive Polling
Subtype	high polling interval
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0

Table 16-37 VNE Switched to Low Polling Rate Due to CPU High Usage (continued)

Service Alarm Setting	Registry Parameter
Northbound metadata	alarm-type=124
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VNE switched to low polling rate due to CPU high usage

Table 16-38 VNE Switched to Maintenance Mode Due to CPU High Usage

Service Alarm Setting	Registry Parameter
Type	Adaptive polling
Subtype	maintenance
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=124
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VNE switched to maintenance mode due to CPU high usage

Table 16-39 VNE Switched Back to Regular Polling Rate

Service Alarm Setting	Registry Parameter
Type	Adaptive polling
Subtype	regular polling interval

Table 16-39 VNE Switched Back to Regular Polling Rate (continued)

Service Alarm Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=124
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=VNE switched back to regular polling rate

All IP Interfaces Down

Table 16-40 Active IP Interface Found

Event Setting	Registry Parameter
Type	All IP interfaces down
Subtype	active ip interfaces found
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=837
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Active ip interfaces found

Table 16-40 Active IP Interface Found (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-41 All IP Interfaces Down

Event Setting	Registry Parameter
Type	all ip interfaces down
Subtype	all ip interfaces down
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=750
Northbound metadata	alarm-type=837
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=All ip interfaces down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

BGP Link Down

Table 16-42 BGP Link Down

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down

Table 16-42 BGP Link Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=599
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down

BGP Link Down VRF

Table 16-43 BGP Link Down VVRF

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down vrf
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=400
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down vrf

BGP Link Up

Table 16-44 BGP Link Up

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BGP link up

BGP Neighbor Loss

Table 16-45 BGP Neighbor Found

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	BGP neighbor found
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 16-45 BGP Neighbor Found (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BGP neighbor found

Table 16-46 BGP Neighbor Loss

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	BGP neighbor loss
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss

Table 16-47 BGP Neighbor Loss VRF

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	bgp-neighbor-loss-vrf

Table 16-47 BGP Neighbor Loss VRF (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=400
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss vrf

BGP Process Down

Table 16-48 BGP Process Down

Event Setting	Registry Parameter
Type	bgp-process-down
Subtype	bgp-process-down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1501
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP process down

Table 16-49 BGP Process Up

Event Setting	Registry Parameter
Type	bgp-process-down
Subtype	bgp-process-up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1501
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BGP process up

Broken LSP Discovered

Table 16-50 Broken LSP Discovered

Event Setting	Registry Parameter
Type	Broken LSP discovered
Subtype	Broken LSP discovered
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=129
	auto-cleared=true
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Broken LSP discovered

Card Down

Table 16-51 Card Down

Event Setting	Registry Parameter
Type	card down
Subtype	card down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=11
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Card down

Table 16-52 Card Up

Event Setting	Registry Parameter
Type	card down
Subtype	card up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=11
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Card up

Card Out

Table 16-53 Card In

Event Setting	Registry Parameter
Type	card out
Subtype	card in
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Card in

Table 16-54 Card Out

Event Setting	Registry Parameter
Type	card out
Subtype	card out
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Card out

Table 16-55 Subcard Out

Event Setting	Registry Parameter
Type	card out
Subtype	subcard out
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Card out

Cloud Problem

Table 16-56 Cloud Problem

Event Setting	Registry Parameter
Type	cloud problem
Subtype	cloud problem
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=2000
Northbound metadata	alarm-type=122
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=INFO
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cloud problem

Table 16-57 Cloud Problem Fixed

Event Setting	Registry Parameter
Type	cloud problem
Subtype	cloud up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=122
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cloud problem fixed

Component Unreachable

Table 16-58 Device Reachable

Event Setting	Registry Parameter
Type	component unreachable
Subtype	component reachable
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Device reachable

Table 16-59 Device Unreachable

Event Setting	Registry Parameter
Type	component unreachable
Subtype	component unreachable
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=600
Northbound metadata	alarm-type=5
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Device unreachable

CPU Utilization

Table 16-60 CPU Normal Utilization

Event Setting	Registry Parameter
Type	cpu utilization
Subtype	cpu normal use
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=17
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=CPU normal utilization

Table 16-61 CPU Overutilized

Event Setting	Registry Parameter
Type	cpu utilization
Subtype	cpu over utilized
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=17
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=CPU over utilized

Device Unsupported

Table 16-62 Device Initializing

Event Setting	Registry Parameter
Type	device unsupported
Subtype	device initializing
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=16
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Device initializing

Table 16-63 Device Unsupported

Event Setting	Registry Parameter
Type	device unsupported
Subtype	device unsupported
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=16
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Device unsupported

Dropped Packets

Table 16-64 Dropped Packets on Port

Event Setting	Registry Parameter
Type	dropped packets
Subtype	dropped packets
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=10
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Dropped packets on port

Table 16-65 Stopped Dropping Packets on Port

Event Setting	Registry Parameter
Type	dropped packets
Subtype	normal dropped packets
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=10
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Stopped dropping packets on port

Discard Packets

Table 16-66 Discard Packets

Event Setting	Registry Parameter
Type	discard packets
Subtype	discard packets
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=9
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Drops exceed limit

Table 16-67 Normal Discard Packets

Event Setting	Registry Parameter
Type	discard packets
Subtype	normal discard packets
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=9
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Drops don't exceed limit

GRE Tunnel Down

Table 16-68 GRE Tunnel Down

Event Setting	Registry Parameter
Type	GRE tunnel down
Subtype	GRE tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=830
Northbound metadata	alarm-type=358
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=GRE tunnel down

Table 16-69 GRE Tunnel Up

Event Setting	Registry Parameter
Type	GRE tunnel down
Subtype	GRE tunnel up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=358
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=GRE tunnel up

HSRP Group Status Changed

Table 16-70 Primary HSRP Interface Is Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Primary HSRP interface is active
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Primary HSRP interface is active

Table 16-71 Primary HSRP Interface Is Not Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Primary HSRP interface is not active
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=720
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Primary HSRP interface is not active

Table 16-72 Secondary HSRP Interface Is Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Secondary HSRP interface is active
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=720
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Secondary HSRP interface is active

Table 16-73 Secondary HSRP Interface Is Not Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Secondary HSRP interface is not active
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Secondary HSRP interface is not active

Interface Status

Table 16-74 Interface Status Down

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down GRE tunnel
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=825
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down

Table 16-74 Interface Status Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-75 Interface Status Down

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down connection
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=500
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-76 Interface Status Down

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down non connection

Table 16-76 Interface Status Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=700
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-77 Interface Status Up

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 16-77 Interface Status Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Interface status up
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Investigation State

Table 16-78 Investigation State

Event Setting	Registry Parameter
Type	investigation state
Subtype	investigation state module unsupported
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=262
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Module unsupported

L2TP Peer Not Established

Table 16-79 l2TP Peer Established

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer established
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp peer established
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-80 l2TP Peer Is Removed

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer is removed
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0

Table 16-80 l2TP Peer Is Removed (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp peer is removed
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-81 l2TP Peer Not Established

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer not established
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=l2tp peer not established

Table 16-81 l2TP Peer Not Established (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

L2tp Sessions Threshold

Table 16-82 l2TP Sessions Count Exceeds Maximum Threshold

Event Setting	Registry Parameter
Type	l2tp sessions threshold
Subtype	l2tp sessions count exceeds max threshold
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=N/A (TCA alarm)
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=l2tp sessions count exceeds max threshold

Table 16-83 l2TP Sessions Count Has Returned To Normal

Event Setting	Registry Parameter
Type	l2tp sessions threshold
Subtype	l2tp sessions count has returned to normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 16-83 l2TP Sessions Count Has Returned To Normal (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=N/A (TCA alarm)
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp sessions count has returned to normal

Layer 2 Tunnel Down

Table 16-84 Layer 2 Tunnel Down

Event Setting	Registry Parameter
Type	layer 2 tunnel down
Subtype	layer 2 tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=179
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Layer 2 tunnel down

Table 16-85 Layer 2 Tunnel Up

Event Setting	Registry Parameter
Type	layer 2 tunnel down
Subtype	layer 2 tunnel up

Table 16-85 Layer 2 Tunnel Up (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=179
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Layer 2 tunnel up

LDP Neighbor Loss

Table 16-86 LDP Neighbor Down

Event Setting	Registry Parameter
Type	LDP neighbor loss
Subtype	LDP neighbor down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=670
Northbound metadata	alarm-type=557
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=LDP neighbor down

Table 16-87 LDP Neighbor Up

Event Setting	Registry Parameter
Type	LDP neighbor loss
Subtype	LDP neighbor up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=557
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=LDP neighbor up

Link Down

Table 16-88 Link Down Due To Admin Down

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to admin down

Table 16-88 Link Down Due To Admin Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-89 Link Down Due To Card Event

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to Card event
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-90 Link Down Due To Oper Down

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to oper down

Table 16-90 Link Down Due To Oper Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to oper down
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-91 Link Down On Unreachable

Event Setting	Registry Parameter
Type	link down
Subtype	link down on unreachable
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=850

Table 16-91 Link Down On Unreachable (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down on unreachable
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-92 Link Up

Event Setting	Registry Parameter
Type	link down
Subtype	link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Link up

Table 16-92 Link Up (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Link Utilization

Table 16-93 Link Overutilized

Event Setting	Registry Parameter
Type	link utilization
Subtype	link over Utilized
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=642
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link over utilized

Table 16-94 Link Utilization Normal

Event Setting	Registry Parameter
Type	link utilization
Subtype	link utilization normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0

Table 16-94 Link Utilization Normal (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=642
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Link utilization normal

Logical Port Down

Table 16-95 Logical Port Down

Event Setting	Registry Parameter
Type	logical port down
Subtype	logical port down
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=198
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Logical port down

Table 16-96 Logical Port Up

Event Setting	Registry Parameter
Type	logical port down
Subtype	logical port up

Table 16-96 Logical Port Up (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=198
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Logical port up

Memory Utilization

Table 16-97 Memory OK

Event Setting	Registry Parameter
Type	memory utilization
Subtype	memory normal use
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=18
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Memory OK

Table 16-98 Memory Overutilized

Event Setting	Registry Parameter
Type	memory utilization
Subtype	memory over utilized
Correlation information	activate-flow=-
	correlate=-
	is-correlation-allowed=-
	weight=-
Northbound metadata	alarm-type=18
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Memory over utilized

MPLS Black Hole Found

Table 16-99 MPLS Black Hole Cleared

Event Setting	Registry Parameter
Type	MPLS Black hole found
Subtype	MPLS Black hole cleared
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=128
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS Black hole cleared

Table 16-100 MPLS Black Hole Found

Event Setting	Registry Parameter
Type	MPLS Black hole found
Subtype	MPLS Black hole found
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=650
Northbound metadata	alarm-type=128
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=WARNING
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS Black hole found

MPLS Interface Removed

Table 16-101 MPLS Interface Added

Event Setting	Registry Parameter
Type	MPLS interface removed
Subtype	MPLS interface added
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=972
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS interface added

Table 16-102 MPLS Interface Removed

Event Setting	Registry Parameter
Type	MPLS interface removed
Subtype	MPLS interface removed
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=700
Northbound metadata	alarm-type=972
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS interface removed

MPLS TE Tunnel Down

Table 16-103 MPLS-TE tunnel Down

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS-TE tunnel down

Table 16-103 MPLS-TE tunnel Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-104 MPLS-TE Tunnel Up

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS-TE tunnel up
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Port Down

Table 16-105 Port Down

Event Setting	Registry Parameter
Type	port down
Subtype	port down

Table 16-105 Port Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Port down
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-106 Port Down Due To Card Event

Event Setting	Registry Parameter
Type	port down
Subtype	port down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=900

Table 16-106 Port Down Due To Card Event (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Port down due to Card event
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 16-107 Port Up

Event Setting	Registry Parameter
Type	port down
Subtype	port up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Port up

Table 16-107 Port Up (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Rx Dormant

Table 16-108 Rx Dormant

Event Setting	Registry Parameter
Type	rx dormant
Subtype	rx dormant
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=378
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=rx dormant

Table 16-109 Rx Dormant Normal

Event Setting	Registry Parameter
Type	rx dormant
Subtype	rx dormant normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 16-109 Rx Dormant Normal (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=378
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=rx dormant normal

Rx Utilization

Table 16-110 Rx Overutilized

Event Setting	Registry Parameter
Type	rx utilization
Subtype	rx over Utilized
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=8
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=RX over utilized

Table 16-111 Rx Utilization Normal

Event Setting	Registry Parameter
Type	rx utilization
Subtype	rx utilization normal

Table 16-111 Rx Utilization Normal (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=8
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=RX utilization normal

Shelf Out

Table 16-112 Shelf In

Event Setting	Registry Parameter
Type	shelf out
Subtype	shelf in
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=33
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Shelf in

Table 16-113 Shelf Out

Event Setting	Registry Parameter
Type	shelf out
Subtype	shelf out
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=110000
Northbound metadata	alarm-type=33
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Shelf out

Tx Dormant

Table 16-114 Tx Dormant

Event Setting	Registry Parameter
Type	tx dormant
Subtype	tx dormant
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=377
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=tx dormant

Table 16-115 Tx Dormant Normal

Event Setting	Registry Parameter
Type	tx dormant
Subtype	tx dormant normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=377
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=tx dormant normal

Tx Utilization

Table 16-116 Tx Overutilized

Event Setting	Registry Parameter
Type	tx utilization
Subtype	tx over Utilized
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=7
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=TX over utilized

Table 16-117 Tx Utilization Normal

Event Setting	Registry Parameter
Type	tx utilization
Subtype	tx utilization normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=7
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=TX utilization normal