CHAPTER 41

Supported Service Alarms

These topics describe the service alarms supported by Cisco ANA:

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 41-42.

  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.

Table 41-1 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 3.7 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 40-7.

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 41-2 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 Interfaces 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 40-9.

ATM IMA Service

The ATM IMA Service alarm is generated by the IMA group. IMA Group Down events are generated when the number of IMA group members is reduced by a user-defined percentage configured in the registry. The severity depends on the percentage of member removed. To avoid false correlations, the events are combined with the IMA group status. An IMA group down generates the highest severity. Other severities are user-defined.

Table 41-3 ATM IMA Service Alarm

Subtype Event Name	Description
IMA Admin Down	Generated when the IMA group is administratively shut down. All the members are correlated to this event.
IMA Oper Down	Generated when the IMA group is operationally down.

Table 41-3 ATM IMA Service Alarm (continued)

Subtype Event Name	Description
High Priority IMA Down	Generated when IMA members are removed based on the user-defined minimum input. Its severity is critical.
Medium Priority IMA Down	Generated when IMA members are removed based on the user-defined minimum input. Its severity is major.
Low Priority IMA Down	Generated when IMA members are removed based on the user-defined minimum input. Its severity is minor.

Correlation

The IMA Admin Down alarm can be the root cause of other events, but other ATM IMA events cannot be root cause of other events. No events are correlated.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See IMA Service (IIMAGroupOid), page 40-4.

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 41-4 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 with 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 40-8.

BGP Neighbor Loss

If BGP connectivity to a specific device in an MPLS VPN network is lost, VPN sites lose connectivity. The VNE models the BGP connection between routers and actively monitors its state. A BGP Neighbor Loss alarm is generated from both sides of the connection when a connectivity loss occurs. Alarms and tickets are issued and impact analysis information displayed.

The correlation engine identifies various faults that affect the BGP connection and reports them as the root cause for the BGP Neighbor Loss alarm, for example, Link Down, CPU Overutilized, and Link Data Loss.

Note BGP Neighbor Loss alarms are not correlated to each other. They are correlated to the root cause of the connectivity loss.

The BGP Neighbor Loss alarm is detected actively by the system, and service alarms are generated. The system also supports BGP neighbor down syslogs.

When the VNE BGP component polls the BGP neighbor status (expedite or normal polling) and finds that an entry for a neighbor no longer exists or its state changed from Established to another state, the BGP component issues a BGP Neighbor Loss alarm. This alarm causes the BGP component to issue a Root Cause Analysis (RCA) correlation flow to find the root cause. If RCA does not find an alarm to correlate, the VNE sends the alarm to the gateway as a ticket.

If a BGP neighbor loss occurs and the BGP component has no other BGP PE links, all VRFs with route entries to the PE as BGP next hops are true-affected. This information is sent as an update to the previous BGP Neighbor Loss alarm.

Table 41-5 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 with 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 40-8.

BGP Process Down

A Cisco ANA query checks the status of the BGP process when the VNE BGP component polls for the status and configuration of its BGP neighbors (expedite or normal polling). If the BGP process is not running, the VNE BGP component issues a BGP Process Down alarm. This alarm is always a ticket and does not try to correlate to other alarms. All BGP Neighbors Down alarms issued in response to the BGP Process Down alarm are correlated to the BGP Process Down ticket.

Table 41-6 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 40-8.

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 41-110.)

A 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:

- 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.

- 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. 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).

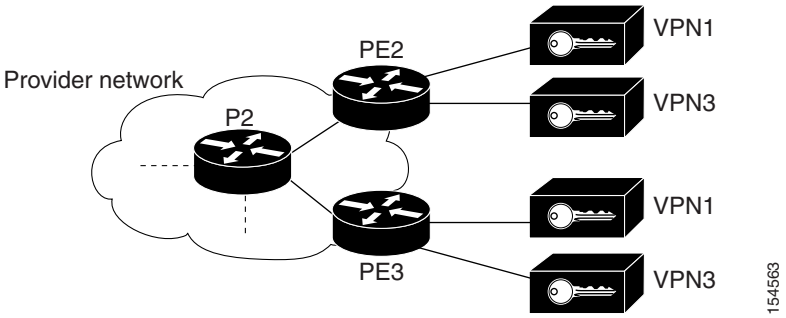
This information is used in the impact analysis process to identify the relevant affected pairs (services).

In the network described in Figure 41-1, the shortest path from PE2 to PE3 is PE2< >P2< >PE3. The link between P2 and PE3 is an MPLS link, meaning interfaces on both sides of the link are configured as MPLS interfaces. Also assume that for some reason, the MPLS configuration is incomplete or incorrect; for example:

- Only one interface is configured as an MPLS interface.
- The label distribution protocol is configured differently on both interfaces (protocol mismatch).

In this case, the label switching table on P2 and PE3 will have untagged entries for the LSPs between PE2 and PE3. If PE2 and PE3 have VPN services (for example VRFs and pseudowires), the outcome will be that the data flow between PE2 and PE3 will be affected.

Figure 41-1 Example of an MPLS Black Hole Scenario



In this case, Cisco ANA does the following:

- Identifies untagged label switching entries on P2 and PE3.
- Issues MPLS Black Hole Found alarms on the interfaces on both sides of the link (since the LSP is unidirectional).
- Initiates a backward flow starting from the link on the specific untagged entries and identifies the two LSPs traversing the link:
  - LSP from PE2 to PE3
  - LSP from PE3 to PE2
- Issues Broken LSP Discovered alarms on both LSPs in PE2 and PE3, which are correlated to the corresponding MPLS Black Hole Found alarm.

Note The clearing alarm does not activate flows to locate the LSPs that were passing through it in order to issue a clearing alarm for Broken LSPs, but rather uses the auto-clear functionality. The gateway periodically reviews the tickets and checks if all the alarms under each ticket are cleared or configured as auto-cleared alarms and whether the gateway correlation timeout has passed, in which case the gateway closes the ticket.

After the MPLS Black Hole alarm clears, and the configured gateway correlation timeout period is reached, the gateway can close the ticket because all the alarms correlated to MPLS Black Hole and Broken LSP are auto-cleared.

Note If an MPLS Network Link Down event causes an IP reroute and an LDP redistribution, new LSPs might be redirected through nonMPLS segments, which will create a black hole. In this case, Broken LSP Discovered alarms are issued. However, the discovered broken LSPs are correlated to the Link Down alarm and not to the MPLS Black Hole Found alarm.

Table 41-7 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 Managed Element OID (IManagedElementOid), page 40-7 (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 41-8 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 40-7.

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 41-9 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 40-7.

CFM Domain Fault

The CFM Domain Fault service alarm is created for every CFM domain having at least one event attached to an entity belonging to that domain (Maintenance Association, Maintenance End Point, and Remote Maintenance End Point). The CFM Domain Fault service alarm is cleared after all the correlated events are cleared.

Events can be aggregated as long as they have a common source OID.

The CFM application is used to aggregate the different CFM syslogs/traps by domain.

The domain OID is contained in the MEP OID.

Table 41-10 CFM Domain Fault

Subtype Event Name	Description
CFM Domain Aggregation Down	Created for every domain having at least one event attached to an entity belonging to the domain: Maintenance Association, Maintenance End Point (MEP), or Remote MEP.
CFM Domain Aggregation Up	Issued after all correlated events are cleared.

Correlation

Because Cisco ANA does not discover CFM topologies, CFM event correlation is not available.

Source OID

IMaintenanceDomainOID

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 41-11 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 find no such alarms, and the flow has traversed a Cloud VNE (a network segment 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 41-13.

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 40-7.

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 41-12 Component Unreachable—Subtype Events

Subtype Event Name	Description
Component 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.
Component 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 40-7 (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 41-13 Unreachable Network Elements

VNE Type	Protocol Used to Check Reachability	Action Taken 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 41-13)Figure 41-1Figure 41-1. 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 representative.

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 40-7.

CPU Utilization

VNEs are configured to trace their device CPU utilization. An alarm is issued when device CPU utilization crosses a configured threshold. The thresholds, as defined in the registry under the managed element, are:

- Upper threshold—80%
- Lower threshold—40%

Table 41-14 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 40-7.

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 41-15 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 40-7.

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 thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—500 packets per second.
- Lower threshold—50 packets per second.

Table 41-16 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 40-9.

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 thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—500 packets per second.
- Lower threshold—50 packets per second.

Table 41-17 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 of 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. It 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 40-9.

DS0 Bundle Service Alarm

DS0 Bundle is a logical interface with an administration and operational status. The DS0Bundle Service alarm is generated when the administration or operational status changes.

Table 41-18 DS0 Bundle Service—Subtype Events

Subtype Event Name	Description
DS0 Bundle Admin Down	Generated when the DS0 Bundle status changes from OK to Admin Down.
DS0 Bundle Oper Down	Generated when the DS0 Bundle status changes from OK to Oper Down.
DS0 Bundle Up	Generated when the DS0 Bundle status changes from Not OK to OK.

Correlation

This alarm will be correlated to lower layer events, such as Port Down. Upper layer events can be correlated to this event.

Source OID

See DS0 Bundle OID (IDS0BundleOid), page 40-2.

DS1 Path Link Down

DS1 Path Link Down is generated when an administrative or operational path shutdown occurs.

Table 41-19 DS1 Path Link Down—Subtype Events

Subtype Event Name	Description
DS1 Path Link Down Due to Admin Down	Generated when the path is administratively shut down.
DS1 Path Link Down Due to Oper Down	Generated when the path is operatively shut down.
DS1 Path Link Up	Generated when the DS1 path is up.

Correlation

DS1 Path Link Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Source OID

See Topological Link OID (ITopologicalLinkOid), page 40-9, where each end point is a DS1 Path OID (IDS1PathOid), page 40-2.

DS1 Path Port Down

DS1 Path Port Down is generated when an administrative or operational path shutdown occurs.

Table 41-20 DS1 Path Port Down—Subtype Events

Subtype Event Name	Description
DS1 Path Port Down	Generated when the DS1 port path is down.
DS1 Path Port Up	Generated when the DS1 port path is up.

Correlation

DS1 Path Port Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Source OID

See DS1 Path OID (IDS1PathOid), page 40-2.

DS3 Path Link Down

DS3 Path Link Down is generated due to administrative or operational shutdown of the path.

Table 41-21 DS3 Path Link Down—Subtype Events

Subtype Event Name	Description
DS3 Path Link Down Due to Admin Down	Generated when the path is administratively shut down.
DS3 Path Link Down Due to Oper Down	Generated when the path is operatively shut down.
DS3 Path Link Up	Generated when the DS1 path is up.

Correlation

DS3 Path Link Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Source OID

See Topological Link OID (ITopologicalLinkOid), page 40-9, where each end point is a DS3 Path OID (IDS3PathOid), page 40-3.

DS3 Path Port Down

DS3 Path Port Down is generated when an administrative or operational path shutdown occurs.

Table 41-22 DS3 Path Port Down—Subtype Events

Subtype Event Name	Description
DS3 Path Port Down	Generated when the DS3 port path is down.
DS3 Path Port Up	Generated when the DS3 port path is up.

Correlation

DS3 Path Port Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Source OID

See DS3 Path OID (IDS3PathOid), page 40-3.

Dual Stack IP Changed

The dual stack IP interface alarm generates events when an interface goes from a dual IP address (IPv4 and IPv6) to a single stack, and when it goes from a single stack to a dual. That is, the event is generated when an IPv6 (global unicast address) or IPv4 address is removed from an interface. The event does not do any correlation but can be a root cause.

Table 41-23 Dual Stack IP Changed

Subtype Event Name	Description
Dual Stack IP Removed	Generated when all IPv6 (global unicast address) or all IPv4 addresses are removed from a dual-stack (two IP addresses) interface.
Dual Stack IP Added	Generated when an IPv6 (global unicast address) or IPv4 address is configured on a single-stack (one IP address) interface that was previously configured as a dual stack.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See IP Interface OID (IPInterfaceOid), page 40-4.

DWDM Controller Down

The DWDM controller has an Up and Admin-Down status. The DWDM Controller Down alarm is generated when the DWDM controller state changes. A DWDM Controller Down ticket is generated. The DWDM Controller Down alarm is based on polling results.

Table 41-24 DWDM Controller Down

Subtype Event Name	Description
DWDM Controller Down	The alarm trigger.
DWDM Controller Up	The clearing alarm.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DWDM Controller OID (IDWDMOid), page 40-3.

DWDM G709 Status Down

The DWDM G709 wrapper has a status of up and down, The DWDM G709 Status Down alarm is generated when the G709 wrapper state changes, and the DWDM G709 Status Down ticket is generated. The alarm is based on the polling result; if the DWDM G709 wrapper status changes, the service alarm is triggered.

Table 41-25 DWDM G709 Status Down

Subtype Event Name	Description
DWDM G709 Status Down	The alarm trigger.
DWDM G709 Status Up	The clearing alarm.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DWDM Controller OID (IDWDMOid), page 40-3.

EFP Down

The EFP Down alarm represents a state in which an Ethernet flow point (EFP) administrative or operational status changes from up to down. The alarm is cleared after the status value is set to up.

The polling of the status property can happen at every standard polling interval, or can be expedited following syslog handling.

The severity of the service alarms is Major, with the exception of EFP Up, which has the severity Cleared.

Table 41-26 EFP Down — Subtype Events

Subtype Event Name	Description
EFP Admin Down	EFP is in administrative status down.
EFP Down Due to Error Disabled	EFT is in operational status down and the error disabled property value is true.
EFP Oper Down	EFP is in operational status down.
EFP Up	Clearing event. Issued when the EFP status returns to up.

Correlation

The generated service alarm searches for its root cause through the correlation mechanism. In addition, the EFP Down alarm is the root cause for every relevant network event caused by the EFP Down event.

Source OID

See EFP OID (IEFPOID), page 40-3.

GRE Keepalive

The GRE Keepalive alarm is generated when the GRE keepalive attribute is not configured or has been removed from a discovered GRE tunnel.

Table 41-27 GRE Keepalive—Subtype Events

Subtype Event Name	Description
Keepalive Not Set	The alarm triggering event when GRE Keepalive is not configured. The event is ticketable with a minor severity.
Keepalive Set	The clearing event.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See GRE Tunnel Endpoint OID Structure, page 40-11.

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 41-28 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 you have chosen to clear and remove 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 40-9 (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 41-29 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.
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 41-29.

Source OID

See IP Interface OID (IPInterfaceOid), page 40-4 (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 41-30.

Table 41-30 Interface Status—Subtype Events

Subtype Event Name	Description
Interface Status Down GRE Tunnel (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 (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 (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 41-30.

Source OID

See IP Interface OID (IPInterfaceOid), page 40-4.

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 41-31 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 40-7.

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 41-32 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 40-4.

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 41-33 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 40-4.

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 41-34 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 40-9 (each endpoint is Layer 2 Mpls Tunnel OID (IPTPMplsLayer2TunnelOid).

LDP Neighbor Loss

LDP enables neighboring P or PE routers acting as LSRs to discover peers in an MPLS network to which they can establish LDP sessions. The sessions allow the routers to negotiate and exchange labels used for forwarding packets.

If a session to an LDP neighbor goes down, an LDP Neighbor Down alarm is issued. This can happen as the result of a failure in the TCP connection used by the LDP session, or if the interface is no longer running MPLS. The LDP neighbor down alarm is cleared by a corresponding LDP Neighbor Up alarm.

The alarm is issued when a peer is removed from the table in the LDP Neighbors tab. The alarm runs a correlation flow to detect the network core triggering event. A root cause analysis is performed to find the root cause. The alarm initiates an IP-based flow toward the peer transport address destination. If an alarm is found during the flow, that alarm is correlated to the LDP Neighbor Down alarm.

Note The LDP Neighbor Down alarm can correlate to the MPLS Interface Removed alarm.

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 41-35 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 40-6 (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 41-37.

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 41-36 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.

Table 41-36 Link Down—Subtype Events (continued)

Subtype Event Name	Description
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

See Topological Link OID (ITopologicalLinkOid), page 40-9 (where each endpoint is Physical Layer OID (IPhysicalLayerOid), page 40-9).

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 41-38 and Tx Utilization, page 41-40.) 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 41-37 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

See Topological Link OID (ITopologicalLinkOid), page 40-9 (where each endpoint is Physical Layer OID (IPhysicalLayerOid), page 40-9).

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 41-38 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 40-5.

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 thresholds, as defined in the registry under ManagedElement, are:

- Upper threshold—80%
- Lower threshold—40%

Table 41-39 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 40-7.

MLPPP Bundle

MLPPP Bundle does not generate a Service alarm for each endpoint; it generate the alarm for links. If a link is not available, the service alarm is generated for individual endpoints. MLPPP Bundle can be a root cause. However, it canot be correlated to other service alarms; that is, another event cannot be the root cause of MLPPP Down. MLPPP Bundle is ticketable.

Table 41-40 MLPPP Bundle Service Alarm

Subtype Event Name	Description
MLPPP Down Due To Flapping	Generated when MLPPP is down due to flapping.
MLPPP Down Flapping Update	Generated when MLPPP flapping update occurs.
MLPPP Down Flapping Proxy	Generated when MLPPP is down due to flapping proxy.
MLPPP Down Due To Admin Down	Generated when MLPPP is administratively shut down on either side.
MLPPP Down Due To Oper Down	Generated when MLPPP is down but neither endpoint is administratively shut down.
MLPPP Up	Generated when either side changes to up.

Correlation

MLPPP Down cannot be correlated to other events. However, other events can correlate to MLPPP Down.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MLPPP OID (IMLPPPOid), page 40-7 or Topological Link OID (ITopologicalLinkOid), page 40-9, where each endpoint is a MLPPP OID (IMLPPPOid), page 40-7.

MPLS Black Hole Found

An MPLS black hole is an abnormal termination of an MPLS path (an LSP) inside an MPLS network. An 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 41-41 MPLS Black Hole 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 41-8.
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 40-6 (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 41-42 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 41-8.
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 40-6 (Label Switching Entity with differentiator object of the MPLS interface description).

MPLS TE FRR State Changed

The MPLS TE FRR State Changed service alarm is triggered when the backup MPLS TE FRR tunnel changes from Ready to Active, and from Active to Ready.

Table 41-43 MPLS TE FRR State Changed

Subtype Event Name	Description
MPLS TE FRR State Changed to Active	Generated when the status of the protecting MPLS TE FRR tunnel changes from Ready to Active because of a network failure in the primary tunnel segment.
MPLS TE FRR State Changed to Ready	Generated when the status of the protecting MPLS TE FRR tunnel changes back to Ready.

Correlation

Correclation is performed.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MPLS TE Tunnel OID (IMplsTETunnelOid), page 40-8.

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 41-44 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 40-8.

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 41-30.

Table 41-45 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 40-9.

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 41-46 Rx Dormant—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 40-9.

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 thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—75%
- Lower threshold—50%

When a 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 41-31.

Table 41-47 Rx Utilization—Subtype Events

Subtype Event Name	Description
Rx Overutilized	Issued when the number of Rx packets on a device 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

By default, impact analysis is not supported 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 40-9.

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 41-48 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 40-9.

Subinterface Down

QinQ technology refers to the nesting of a VLAN header in an Ethernet frame in an already existing VLAN header. Both VLAN headers must be of the type 802.1Q. When one VLAN header is nested within another VLAN header, they are often referred to as *stacked VLANs*. QinQ technology allows service provider networks to carry traffic with double-tagged, stacked VLAN (802.1Q-in-Q) headers of multiple customers while maintaining the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

A subinterface is a logical division of traffic on an interface, such as multiple subnets across one physical interface. A subinterface name is represented as an extension to an interface name using dot notation, such as Interface Gigabit Ethernet 0/1/2/3.10. In this example, the main interface name is Gigabit Ethernet 0/1/2/3 and the subinterface is 10.

A Subinterface Down alarm is issued when the administrative or operational state of an Ethernet subinterface of a stacked VLAN changes. This state can be polled at standard polling intervals or can be expedited following syslog handling.

Table 41-49 Subinterface Down—Subtype Events

Subtype Event Name	Description
Subinterface Down	Issued when the operational status of the subinterface changes from up to down.
Subinterface Admin Down	Issued when the administrative status of the subinterface changes from up to down.
Subinterface Up	Clearing event. Issued when the operational or administrative status of the subinterface changes from down to up.

Correlation

The Subinterface Down event searches for the root cause through the correlation mechanism. The Subinterface Admin Down event does not search for the root cause through the correlation mechanism.

Subinterface Down is the root cause for every relevant network event caused by the Subinterface Down event.

Source OID

See VLAN Tagged Interface OID (IVlanTaggedInterfaceOID), page 40-12.

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 PortLayer1.

Note This alarm is disabled by default.

Table 41-50 Tx Dormant—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 40-9.

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 thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—75%
- Lower threshold—50%

When a 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 41-31.

Table 41-51 Tx Utilization—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

By default, impact analysis is not supported 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 40-9.

VSI Down

The VSI Down alarm represents a state in which a virtual switch instance (VSI) administrative or operational status changes from up to down. The alarm is cleared after the status value is set to up.

The polling of the status property can happen at every standard polling interval, but it can be expedited following the trap handling of one of the following:

- VLAN interface status change of a VLAN that is connected to a VSI.
- Pseudowire status change of a pseudowire configured on the VSI.

The severity of the service alarms is Major, except for VSI Admin Down alarm.

Table 41-52 VSI Down —Subtype Events

Subtype Event Name	Description
VSI Down	VSI is in operational status down.
VSI Admin Down	VSI is in administrative status down.
VSI Up	VSI status is up.

Correlation

The VSI Down alarm does not start a correlation process and is always issued as a root cause alarm.

Source OID

See VSI OID (IVSIOID), page 40-12.

Registry Parameters

The following registry parameters are included in this section:

Adaptive Polling

Table 41-53 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
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 41-54 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 41-55 VNE Switched Back to Regular Polling Rate

Service Alarm Setting	Registry Parameter
Type	Adaptive polling
Subtype	regular polling interval
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 41-56 Active IP Interfaces 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
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-57 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

Table 41-57 All IP Interfaces Down (continued)

Event Setting	Registry Parameter
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

ATM IMA Down

Table 41-58 IMA Admin Down

Event Setting	Registry Parameter
Type	IMA Down
Subtype	IMA Admin Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=110000

Table 41-58 IMA Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=681
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=ima administratively down

Table 41-59 IMA Oper Down

Event Setting	Registry Parameter
Type	IMA Down
Subtype	IMA Oper Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ima operationally down

Table 41-60 High Priority IMA Down

Event Setting	Registry Parameter
Type	IMA Down
Subtype	High Priority IMA Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=high priority ima down

Table 41-61 Medium Priority IMA Down

Event Setting	Registry Parameter
Type	IMA Down
Subtype	Medium Priority IMA Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800

Table 41-61 Medium Priority IMA Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=high priority ima down

Table 41-62 Low Priority IMA Down

Event Setting	Registry Parameter
Type	IMA Down
Subtype	Low Priority IMA Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=high priority ima down

BGP Link Down

Table 41-63 BGP Link Down

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down
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 41-64 BGP Link Down VRF

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

Table 41-64 BGP Link Down VRF (continued)

Event Setting	Registry Parameter
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 41-65 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 41-66 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
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 41-67 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 41-68 BGP Neighbor Loss VRF

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	bgp-neighbor-loss-vrf
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 41-69 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 41-70 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 41-71 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 41-72 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 41-73 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 41-74 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 41-75 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 41-76 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

CFM Domain Fault

Table 41-77 CFM Domain Aggregation Down

Event Setting	Registry Parameter
Type	CFM Domain Fault
Subtype	CFM Domain Aggregation Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=2
Northbound metadata	alarm-type=3016
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=9223372036854775807
	is-ticketable=true
	priority=0

Table 41-77 CFM Domain Aggregation Down (continued)

Event Setting	Registry Parameter
	reduction-counter=1
	send-to-gw=true
	severity=INFO
	short-description=CFM Domain fault

Table 41-78 CFM Domain Aggregation Up

Event Setting	Registry Parameter
Type	CFM Domain Fault
Subtype	CFM Domain Aggregation Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=3016
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=CFM Domain fault cleared

Cloud Problem

Table 41-79 Cloud Problem

Event Setting	Registry Parameter
Type	cloud problem
Subtype	cloud problem

Table 41-79 Cloud Problem (continued)

Event Setting	Registry Parameter
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 41-80 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 41-81 Component 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 41-82 Component 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 41-83 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 41-84 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 41-85 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 41-86 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

Discard Packets

Table 41-87 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 41-88 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

Dropped Packets

Table 41-89 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 41-90 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

DSO Bundle

Table 41-91 DS0 Bundle Admin Down

Event Setting	Registry Parameter
Type	DSO Bundle Down
Subtype	DSO Bundle Admin Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=750
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle admin down

Table 41-92 DS0 Bundle Oper Down

Event Setting	Registry Parameter
Type	DSO Bundle Down
Subtype	DSO Bundle Oper Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=725

Table 41-92 DS0 Bundle Oper Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle oper down

Table 41-93 DS0 Bundle Up

Event Setting	Registry Parameter
Type	DSO Bundle Down
Subtype	DSO Bundle Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-93 DS0 Bundle Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=ds0 bundle up

DS1 Path Link Down

Table 41-94 DS1 Path Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	DS1 Path Link Down
Subtype	DS1 Path Link Admin Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=815

Table 41-94 DS1 Path Link Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down due to admin down

Table 41-95 DS1 Path Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	DS1 Path Link Down
Subtype	DS1 Path Link Oper Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=810

Table 41-95 DS1 Path Link Down Due to Oper Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down due to oper down

Table 41-96 DS1 Path Link Up

Event Setting	Registry Parameter
Type	DS1 Path Link Down
Subtype	DS1 Path Link Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-96 DS1 Path Link Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS1 Path Link up

DS1 Path Port Down

Table 41-97 DS1 Path Port Down

Event Setting	Registry Parameter
Type	DS1 Path Port Down
Subtype	DS1 Path Port Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=810

Table 41-97 DS1 Path Port Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1322
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down

Table 41-98 DS1 Path Port Up

Event Setting	Registry Parameter
Type	DS1 Path Port Down
Subtype	DS1 Path Port Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-98 DS1 Path Port Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1322
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS1 Path up

DS3 Path Link Down

Table 41-99 DS3 Path Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	DS3 Path Link Down
Subtype	DS3 Path Link Admin Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=825

Table 41-99 DS3 Path Link Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down due to admin down

Table 41-100 DS3 Path Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	DS3 Path Link Down
Subtype	DS3 Path Link Oper Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=820

Table 41-100 DS3 Path Link Down Due to Oper Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down due to oper down

Table 41-101 DS3 Path Link Up

Event Setting	Registry Parameter
Type	DS3 Path Link Down
Subtype	DS3 Path Link Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-101 DS3 Path Link Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS3 Path up

DS3 Path Port Down

Table 41-102 DS3 Path Port Down

Event Setting	Registry Parameter
Type	DS3 Path Port Down
Subtype	DS3 Path Port Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=820

Table 41-102 DS3 Path Port Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle admin down

Table 41-103 DS3 Path Port Up

Event Setting	Registry Parameter
Type	DS3 Path Port Down
Subtype	DS3 Path Port Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-103 DS3 Path Port Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle oper down

Dual Stack IP Changed

Table 41-104 Dual Stack IP Removed

Event Setting	Registry Parameter
Type	Dual stack IP changed
Subtype	Dual stack IP removed
Correlation information	activate-flow=true
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=820

Table 41-104 Dual Stack IP Removed (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1170
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=Dual stack IP removed

Table 41-105 Dual Stack IP Added

Event Setting	Registry Parameter
Type	DS3 Path Port Down
Subtype	DS3 Path Port Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-105 Dual Stack IP Added (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1170
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=Dual stack IP added

DWDM Controller

Table 41-106 DWDM Controller Down

Event Setting	Registry Parameter
Type	DWDM Controller
Subtype	DWDM Controller Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-106 DWDM Controller Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1888
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=dwdm controller down

Table 41-107 DWDM Controller Up

Event Setting	Registry Parameter
Type	DWDM Controller
Subtype	DWDM Controller Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-107 DWDM Controller Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1888
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=dwdm controller up

DWDM G709 Status

Table 41-108 DWDM G709 Status Down

Event Setting	Registry Parameter
Type	DWDM G709 Status
Subtype	DWDM G709 Status Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-108 DWDM G709 Status Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1889
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=dwdm g709 status down

Table 41-109 DWDM G709 Status Up

Event Setting	Registry Parameter
Type	DWDM G709 Status
Subtype	DWDM G709 Status Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-109 DWDM G709 Status Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1889
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=dwdm g709 status up

EFP Down

Table 41-110 EFP Admin Down

Event Setting	Registry Parameter
Type	efp down
Subtype	efp admin down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=EFP Down

Table 41-111 EFP Down Due to Error Disabled

Event Setting	Registry Parameter
Type	efp down
Subtype	efp down due to error disabled
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=EFP down due to error disabled

Table 41-112 EFP Oper Down

Event Setting	Registry Parameter
Type	efp down
Subtype	efp oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=EFP down

Table 41-113 EFP Up

Event Setting	Registry Parameter
Type	efp down
Subtype	efp up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=EFP up

GRE Keepalive

Table 41-114 Keepalive Not Set

Event Setting	Registry Parameter
Type	Keepalive
Subtype	Keepalive not set
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 41-114 Keepalive Not Set (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=915
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=Keepalive not configured

Table 41-115 Keepalive Set

Event Setting	Registry Parameter
Type	Keepalive
Subtype	Keepalive set
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=915
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=Keepalive configured

GRE Tunnel Down

Table 41-116 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 41-117 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 41-118 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 41-119 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 41-120 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 41-121 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 41-122 Interface Status Down GRE Tunnel

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
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-123 Interface Status Down Connection

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

Table 41-123 Interface Status Down Connection (continued)

Event Setting	Registry Parameter
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 41-124 Interface Status Down Nonconnection

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

Table 41-124 Interface Status Down Nonconnection (continued)

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

Table 41-125 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
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 41-126 Investigation State

Event Setting	Registry Parameter
Type	investigation state
Subtype	investigation state module unsupported

Table 41-126 Investigation State (continued)

Event Setting	Registry Parameter
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 41-127 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

Table 41-127 L2TP Peer Established (continued)

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

Table 41-128 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
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 41-129 L2TP Peer Not Established

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer not established

Table 41-129 L2TP Peer Not Established (continued)

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

L2TP Sessions Threshold

Table 41-130 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

Table 41-130 L2TP Sessions Count Exceeds Maximum Threshold (continued)

Event Setting	Registry Parameter
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 41-131 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
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 41-132 Layer 2 Tunnel Down

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

Table 41-132 Layer 2 Tunnel Down (continued)

Event Setting	Registry Parameter
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=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Layer 2 tunnel down

Table 41-133 Layer 2 Tunnel Up

Event Setting	Registry Parameter
Type	layer 2 tunnel down
Subtype	layer 2 tunnel up
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 41-134 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 41-135 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 41-136 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
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-137 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

Table 41-137 Link Down Due to Card Event (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 due to Card event
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-138 Link Down Due to Oper Down

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

Table 41-138 Link Down Due to Oper Down (continued)

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

Table 41-139 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
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 41-140 Link Up

Event Setting	Registry Parameter
Type	link down
Subtype	link up

Table 41-140 Link Up (continued)

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

Link Utilization

Table 41-141 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

Table 41-141 Link Overutilized (continued)

Event Setting	Registry Parameter
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 41-142 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
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 41-143 Logical Port Down

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

Table 41-143 Logical Port Down (continued)

Event Setting	Registry Parameter
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 41-144 Logical Port Up

Event Setting	Registry Parameter
Type	logical port down
Subtype	logical port up
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 41-145 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 41-146 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

MLPPP Bundle

Table 41-147 MLPPP Down Due To Flapping

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp down due to flapping
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp down flapping

Table 41-148 MLPPP Down Flapping Update

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp down flapping update
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000

Table 41-148 MLPPP Down Flapping Update (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp down flapping update

Table 41-149 MLPPP Down Due To Admin Down

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp down due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=mlppp administratively down

Table 41-150 MLPPP Down Flapping Proxy

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp down flapping proxy
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=false
	severity=INFO
	short-description=mlppp down flapping proxy

Table 41-151 MLPPP Down Due To Oper Down

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp down due to oper down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000

Table 41-151 MLPPP Down Due To Oper Down (continued) (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp operationally down

Table 41-152 MLPPP Up

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=mlppp up

MPLS Black Hole Found

An MPLS black hole is defined as an abnormal termination of an MPLS path (LSP) inside an MPLS network. An MPLS black hole exists when on a specific interface there are untagged entries destined for a known PE router. It is assumed that a router functions as a PE router if services, such as L3 VPNs or pseudowire (L2 VPN) MPLS tunnels, are using the MPLS network. Note that the untagged interfaces may exist in the network in normal situations; for example, where the boundary of the MPLS cloud has untagged interfaces.

An MPLS black hole causes the loss of all MPLS labels on a packet, including the VPN information that lies in the inner MPLS label. If a packet goes through an untagged interface, the VPN information is lost. The VPN information loss causes VPN sites to lose connectivity.

MPLS Black Hole Found alarms are actively detected. Service alarms are generated whenever Cisco ANA discovers an MPLS interface with at least one untagged LSP leading to a known PE router.

Black hole alarms are detected either:

- When the system is loaded for the first time and performs the initial discovery of the network.
- Through the ongoing discovery process, which identifies changes in the network.

Note MPLS black hole discovery is supported only when the PEs are managed by Cisco ANA.

Table 41-153 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 41-154 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 41-155 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 41-156 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 FRR State Changed

Table 41-157 MPLS TE FRR State Changed to Active

Event Setting	Registry Parameter
Type	mpls te frr state changed
Subtype	mpls te frr state changed to active
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=700

Table 41-157 MPLS TE FRR State Changed to Active (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1322
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=MPLS TE FRR State Changed to Active

Table 41-158 MPLS TE FRR State Changed to Ready

Event Setting	Registry Parameter
Type	mpls te frr state changed
Subtype	mpls te frr state changed to ready
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 41-158 MPLS TE FRR State Changed to Ready (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1322
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=MPLS TE FRR State Changed to Ready

MPLS TE Tunnel Down

MPLS TE tunnel alarms include:

- MPLS TE Tunnel Down
- MPLS TE Tunnel Flapping
- Tunnel Reoptimized

If a TE tunnel operational status changes to down, an MPLS TE Tunnel Down alarm is generated. The Cisco ANA correlation engine identifies the faults that affect the TE tunnel status and identifies the root cause for the MPLS TE Tunnel Down alarm. For example, a Link Down will cause a TE tunnel to go down. Multiple up and down alarms that are generated during a short time interval are suppressed and displayed as an MPLS TE Tunnel Flapping alarm (according to the specific flapping configuration).

MPLS TE Tunnel Down and MPLS TE Tunnel Flapping alarms are actively detected and service alarms are generated. The system also supports MPLS TE Tunnel Down syslogs, which are correlated to the service alarm.

For Cisco CRS-1 routers running Cisco IOS XR 3.6 software and using PBTS in MPLS or MPLS VPN networks, Cisco ANA supports the following subalarms for the MPLE TE Tunnel Down alarm:

- High Priority MPLS TE Tunnel Down
- Medium Priority MPLS TE Tunnel Down
- Low Priority MPLS TE Tunnel Down

The specific subalarm that is generated depends on the EXP bit specified for the traffic. Cisco ANA maps the specified EXP bit to tunnel priority and uses that mapping to generate the resultant subalarm. The alarm description includes information about the EXP bit.

Tunnel reoptimization occurs when a tunnel is up and its route changes but the tunnel continues to remain up. When a TE tunnel is reoptimized to take a different path, the system parses the tunnel reoptimized syslog, if such a syslog is available, and displays it as a ticket.

The Tunnel Reoptimized alarm is generated from a syslog message sent by the router.

Table 41-159 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
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-160 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

Table 41-160 MPLS TE Tunnel Up (continued)

Event Setting	Registry Parameter
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 41-161 Port Down

Event Setting	Registry Parameter
Type	port down
Subtype	port down
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

Table 41-161 Port Down (continued)

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

Table 41-162 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
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 41-163 Port Up

Event Setting	Registry Parameter
Type	port down
Subtype	port up

Table 41-163 Port Up (continued)

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

Rx Dormant

Table 41-164 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

Table 41-164 Rx Dormant (continued)

Event Setting	Registry Parameter
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 41-165 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
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 41-166 Rx Overutilized

Event Setting	Registry Parameter
Type	rx utilization
Subtype	rx over Utilized

Table 41-166 Rx Overutilized (continued)

Event Setting	Registry Parameter
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 41-167 Rx Utilization Normal

Event Setting	Registry Parameter
Type	rx utilization
Subtype	rx utilization normal
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 41-168 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 41-169 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

Subinterface Down

Table 41-170 Subinterface Down

Event Setting	Registry Parameter
Type	subinterface down
Subtype	subinterface oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Subinterface down

Table 41-171 Subinterface Admin Down

Event Setting	Registry Parameter
Type	sub-interface down
Subtype	sub-interface admin down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Sub-Interface down

Table 41-172 Subinterface Up

Event Setting	Registry Parameter
Type	sub-interface down
Subtype	sub-interface up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Sub-Interface up

Tx Dormant

Table 41-173 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 41-174 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 41-175 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 41-176 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

VSI Down

Table 41-177 VSI Down

Event Setting	Registry Parameter
Type	vsi down
Subtype	vsi oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=845
Northbound metadata	alarm-type=916
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VSI down

Table 41-178 VSI Admin Down

Event Setting	Registry Parameter
Type	vsi down
Subtype	vsi admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=101
Northbound metadata	alarm-type=916
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VSI down

Table 41-179 VSI Up

Event Setting	Registry Parameter
Type	vsi down
Subtype	vsi up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=916
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=VSI up