CHAPTER 6

Fault Management In MPLS Networks

This chapter describes the alarms that Cisco ANA detects and reports for LDP, BGP, MPLS TE (using RSVP TE), MPLS Black Holes, as well as alarm reports for Layer 2 and Layer 3 VPNs:

- MPLS Related Faults, page 6-2—Describes the “MPLS black hole found” and “Broken LSP discovered” alarms.
- LDP Related Faults, page 6-4—Describes the “LDP neighbor down” alarm.
- BGP Related Faults, page 6-4—Describes the “BGP neighbor loss” alarm.
- Traffic Engineering Faults, page 6-5—Describes the “MPLS TE tunnel down”, “MPLS TE tunnel flapping” and “Tunnel reoptimized” alarms.
- Layer 2 VPN Faults, page 6-6—Describes the “Pseudo Wire (L2 VPN) MPLS tunnel down” alarm.
- Alarms Summary, page 6-7—Provides a brief description of the alarms for VPNs, including their severity and the up alarm (clearing alarm) for each.

Cisco ANA supports the following alarms:

- MPLS Related Faults:
  - MPLS black hole found
  - Broken LSP discovered
- LDP Related Faults:
  - LDP neighbor down
- BGP Related Faults:
  - BGP neighbor loss
- Traffic Engineering Faults:
  - MPLS TE tunnel down
  - MPLS TE tunnel flapping
  - Tunnel reoptimized
- Layer 2 VPN Faults:
  - Pseudo Wire (L2 VPN) MPLS tunnel down

The alarms are displayed in the ticket pane of the Cisco ANA NetworkVision window. For more information about the ticket pane, see the *Cisco Active Network Abstraction 3.6.5 User Guide*.

MPLS Related Faults

This section includes descriptions of the following MPLS related faults:

- MPLS black hole found
- Broken LSP discovered

Note The MPLS black hole feature is only supported when the PEs are managed by the system.

MPLS Black Hole Found Alarm

A MPLS “black hole” is defined as an abnormal termination of a MPLS path (LSP) inside a MPLS network. A 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 there are services using the MPLS network, such as L3 VPNs or Pseudo Wire (L2 VPN) MPLS Tunnels. 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 this is still considered normal.

The existence of a MPLS “black hole” results in a loss of all the MPLS labels on a packet including the VPN information which lies in the inner MPLS label. So if a packet goes through an untagged interface, the VPN information is lost. The VPN information loss translates directly to VPN sites losing connectivity.

A “MPLS Black Hole Found” alarm is detected actively by the system, namely, service alarms are generated whenever Cisco ANA discovers a MPLS interface that has 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.

Broken LSP Discovered Alarm

The “MPLS Black Hole Found” alarm activates a backward flow on the specific untagged entry in order to traverse the full path of the LSPs passing through it. If Cisco ANA locates services (VRFs, Pseudo Wire L2 tunnels) along this path that are using these LSPs a “Broken LSP Discovered” alarm is issued. Such services can only be found on PE routers and they can be found on more than one PE router. The source of the “Broken LSP Discovered” alarm is the PE router on which the service was discovered and in many cases this router is different from the router that issued the “MPLS Black Hole Found” alarm.

“Broken LSP Discovered” alarms are correlated to the “MPLS Black Hole Found” alarm (except in the case of a Black hole alarm due to a link down as described on page 6-4).

The “Broken LSP Discovered” alarm is detected actively by the system, namely, service alarms are generated.

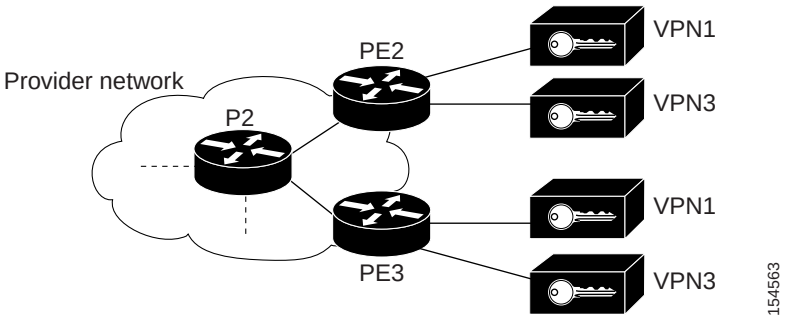
An example of a MPLS black hole scenario follows.

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

- Only one interface is configured as a 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 (VRFs, Pseudo Wire tunnels) the outcome will be that the data flow between PE2 and PE3 will be affected.

Figure 6-1 Example of a 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 2 LSPs traversing the link, namely:
  - 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, and in this case the Gateway closes the ticket.

Using this functionality, once the "MPLS Black hole" alarm is cleared, then after a specific time interval (configured Gateway correlation timeout) has passed, the Gateway will be able to close the ticket since all the alarms correlated to "MPLS Black hole" are "Broken LSP" which are configured as auto cleared.

Black Hole To Link Down

In a case where a link down event in a MPLS network has caused an IP reroute and therefore LDP redistribution, a case may arise where new LSPs are now redirected through a non-MPLS segment thereby creating a black hole.

In this case the “Broken LSP Discovered” alarms are issued as described in Broken LSP Discovered Alarm, page 6-2, but all the broken LSPs that are found are correlated to the “Link Down” alarm and not to the “MPLS Black Hole Found” alarm.

LDP Related Faults

Label Distribution Protocol (LDP) enables neighboring P or PE routers acting as label switch routers (LSRs) to discover potential peers in an MPLS network with which they can establish LDP sessions, in order to negotiate and exchange labels to be 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 what event happened in the network core, and then performs a Root Cause Analysis to find its root cause. The alarm initiates an IP based flow towards the “Peer Transport Address" destination. If an alarm is found during the flow, it will correlate to it.

Note The "LDP neighbor down" alarm can correlate to the “MPLS interface removed" alarm.

BGP Related Faults

Cisco ANA monitors BGP neighbor information and makes correlation and impact analysis information available to users.

This section includes a description of the BGP related faults.

BGP Neighbor Loss

In IP/MPLS VPN networks, when BGP connectivity is lost to a specific device, the resulting BGP connection loss translates directly to VPN sites losing 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 in the case of a connectivity loss, resulting in alarms and tickets being issued and users viewing impact analysis information.

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 over utilized, and Link data loss.

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

The "BGP Neighbor Loss" alarm is detected actively by the system, namely, service alarms are generated.

The system also supports "BGP neighbor down" syslogs.

BGP Neighbor Loss

When the VNE's BGP component is polling the status of BGP neighbors (expedite or normal polling), and an entry for a neighbor does not exist any more or its state changed from Established state to any other state, the BGP component will issue an alarm for "BGP Neighbor Loss". This alarm causes the BGP component to issue a Root Cause Analysis (RCA) correlation flow to find its root cause.

If RCA does not find any alarm to correlate to, the VNE will send this alarm to the gateway as a ticket.

If this alarm is configured in the registry to issue "Look For Affected" flow, the following process will be issued:

- For each BGP link, the BGP component holds a list of PE routers (routers with VRFs) that it can reach.
- If there is a BGP neighbor loss and the BGP component has no other BGP link to a PE, all VRFs on this device with route entries with that PE as BGP next hop will be true affected.
- This information will be sent as an update for the previous "BGP Neighbor Loss" alarm.

BGP Process Down

A query checks the status of the BGP process when the VNE's BGP component is polling for the status and configuration of its BGP neighbors (expedite or normal polling).

If the BGP process is not running, the VNE's BGP component will issue an alarm "BGP Process Down".

This alarm will always be a ticket and will not try to correlate to other alarms.

All the "BGP Neighbors Down" alarms issued due to the "BGP Process Down" should correlate to this "BGP Process Down" ticket.

Traffic Engineering Faults

This section includes a description of the following Traffic Engineering related faults:

- MPLS TE tunnel down
- MPLS TE tunnel flapping
- Tunnel reoptimized

MPLS TE Tunnel Down and TE Tunnel Flapping

When a TE tunnel's operational status changes to down and the tunnel is not flapping, the system generates a "Tunnel Down" alarm.

The correlation engine identifies various faults that affect the TE tunnel's status and reports on them as the root cause for the TE "Tunnel Down" alarm, for example, Link down.

Multiple up and down alarms that are generated during a short time interval are suppressed and displayed as a "Tunnel Flapping" alarm (according to the specific flapping configuration).

The "MPLS TE Tunnel Down" and the "TE Tunnel flapping" alarms are detected actively by the system, namely, 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 3 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 Reoptimized

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 this syslog as a ticket.

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

Layer 2 VPN Faults

This section includes a description of the Layer 2 VPN fault, Pseudo Wire (L2 VPN) MPLS tunnel down.

Pseudo Wire (L2 VPN) MPLS Tunnel Down

A "Pseudo Wire MPLS Tunnel Down" alarm is issued when the pseudo wire link goes down, namely, the pseudo wire tunnel is reported as down from both the devices (based on the status of the tunnel), and the tunnel is not flapping.

The correlation engine identifies various faults that affect the Pseudo Wire tunnel status and reports on them as the root cause for the "Pseudo Wire MPLS Tunnel Down" alarm, for example, Link down.

Cisco ANA traces the LSE path to the edge of the **PWE3** tunnel and marks the edges of the tunnel as affected.

The "Pseudo Wire MPLS Tunnel Down" alarm is detected actively by the system, namely, service alarms are generated.

Alarms Summary

The following section describes the alarms that may be displayed in the ticket pane of the Cisco ANA NetworkVision window for VPNs, including their severity and the up alarm for each:

Table 6-1 Alarms Displayed In the Ticket Pane

Alarm	Default Severity	Description	Up Alarm
BGP Neighbor Loss	Red (critical)	The “BGP Neighbor Loss” alarm is generated whenever BGP connectivity is lost to a specific device.	BGP Neighbor Found
LDP Neighbor Down	Orange (major)	The “LDP Neighbor Down” alarm is generated whenever there is a failure in the TCP connection on which LDP is running, or if the interface is no longer running MPLS.	LDP Neighbor Up
MPLS Black Hole Found	Dark blue (information)	A “MPLS Black Hole Found” alarm is generated whenever Cisco ANA discovers a MPLS interface that has at least one untagged LSP leading to a known PE router.	MPLS Black Hole Cleared
Broken LSP Discovered	Orange (major)	The “MPLS Black Hole Found” alarm activates a backward flow on the specific untagged entry in order to traverse the full path of the LSPs passing through it. The “Broken LSP Discovered” alarm is generated whenever Cisco ANA locates services (VRFs, Pseudo Wire L2 tunnels) along this path that are using these LSPs.	N/A
MPLS TE Tunnel Down	Orange (major)	The “MPLS TE Tunnel Down” alarm is generated whenever a TE tunnel’s operational status changes to down and the tunnel is not flapping.	MPLS TE Tunnel Up
MPLS TE Tunnel Flapping	Orange (major)	The “TE Tunnel flapping” alarm is generated whenever multiple up and down alarms are generated during a short time interval and they are suppressed.	Is the last state of the tunnel after it has stopped flapping
Pseudo Wire (L2 VPN) MPLS Tunnel Down	Yellow (minor)	The “Pseudo Wire MPLS Tunnel Down” alarm is generated whenever the pseudo wire link goes down, namely, the pseudo wire tunnel is reported as down from both the devices (based on the status of the tunnel).	Layer 2 Tunnel Up
Tunnel Reoptimized	Dark Blue (information)	The “Tunnel Reoptimized” alarm is generated from a syslog message sent by the router whenever a tunnel is up and its route changes but the tunnel continues to remain up.	N/A

For more information about the ticket pane, see the *Cisco Active Network Abstraction 3.6.5 User Guide*.