CHAPTER 6

Fault Management in MPLS Networks

The following topics describes the alarms that Cisco MPLS Assurance Manager 1.0 (Cisco MPLS-AM) detects and reports for supported MPLS-related services. The following sections describe the MPLS VPNs, BGP, TE tunnel,and pseudowire alarms:

Overview

Cisco MPLS-AM supports alarms related to Multiprotocol Label Switching (MPLS) protocol, the Border Gateway Protocol (BGP) protocol, Traffic Engineering (TE) tunnels, and pseudowires. The alarms are displayed in the Active Tickets tab in the Cisco Active Network Abstraction 4.0 (ANA) Inventory and Monitoring perspectives Common Supporting View (CSV). Detailed alarm information is viewed in the Troubleshooting perspective. Table 6-1 shows the MPLS, BGP, TE tunnel, and pseudowire alarms supported by Cisco MPLS-AM. For more information about viewing and managing alarms in ANA, see the *Cisco Active Network Abstraction 4.0 User and Administration Guide*.

Table 6-1 MPLS, BGP, TE Tunnel, and Pseudowire Alarms

Alarm	Area	Default Severity	Description	Up Alarm
MPLS Black Hole Found	MPLS	Warning	A MPLS Black Hole Found alarm is generated by a provider core (P) or provider edge (PE) router virtual network element (VNE) whenever Cisco MPLS-AM discovers a MPLS interface that has at least one untagged label switched path (LSP) leading to a known PE VNE.	MPLS Black Hole Cleared
Broken LSP Discovered	MPLS	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 MPLS-AM locates services (VRFs, pseudowire L2 tunnels) along this path that are using these LSPs.	N/A

Table 6-1 MPLS, BGP, TE Tunnel, and Pseudowire Alarms (continued)

Alarm	Area	Default Severity	Description	Up Alarm
BGP Neighbor Loss	BGP	Critical	The BGP Neighbor Loss alarm is generated whenever BGP connectivity is lost to a specific device.	BGP Neighbor Found
MPLS TE Tunnel Down	TE Tunnel	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	TE Tunnel	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.	The last state of the tunnel after it stops flapping
Layer 2 Tunnel Down	Pseudowire	Major	The Pseudowire MPLS Tunnel Down alarm is generated whenever the pseudowire link goes down, namely, the pseudowire tunnel is reported as down from both the devices (based on the status of the tunnel).	Layer 2 Tunnel Up

MPLS Fault Management

This section describes MPLS faults. Alarms raised by MPLS faults include:

- MPLS Black Hole Found Alarm
- Broken LSP Discovered Alarm

Note The MPLS black hole alarms only appear when the PEs are managed by the system.

MPLS Black Hole Found Alarm

An MPLS "black hole" is an abnormal termination of a label switched path (LSP) from a P or PE device inside an MPLS network. An MPLS black hole occurs when untagged entries destined for a known PE accumulate on a specific interface. The assumption is the router functions as a PE when services using the MPLS network exist, such as L3 VPNs, TE tunnels, or pseudowires.

Note Untagged interfaces might exist in a network in normal situations. For example, where the boundary of the MPLS cloud has untagged interfaces, untagged interfaces are considered normal.

An MPLS black hole causes packets to lose their MPLS labels 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 and VPN sites lose connectivity. An MPLS Black Hole Found alarm is raised whenever Cisco MPLS-AM discovers an MPLS interface that has at least one untagged LSP leading to a known PE router. Black hole detection occurs when the system is loaded for the first time and performs the initial discovery of the network. It also occurs during 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 untagged entry to trace the full path of the LSPs passing through it. If Cisco MPLS-AM finds VRFs, pseudowires, or other MPLS services along the path that use the LSPs, a Broken LSP Discovered alarm is issued. These services can only be found on PEs, and usually on more than one PE.

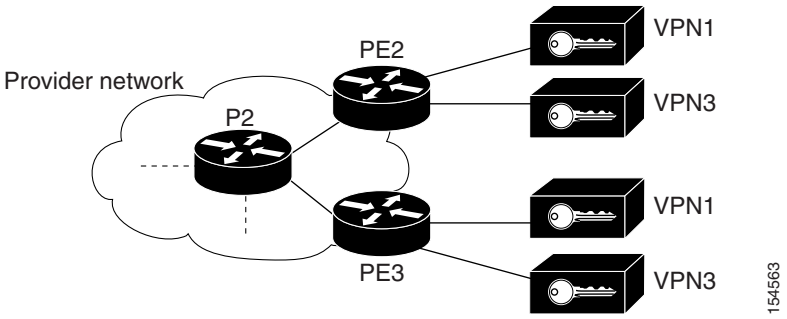
Broken LSP Discovered alarms are correlated to the MPLS Black Hole Found alarm. Figure 6-1 shows an example of an MPLS network. In the example, the shortest path from PE2 to PE3 is PE2 <-> P2 <-> PE3. The link between P2 and PE3 is an MPLS link, so the interfaces on both sides of the link are configured as MPLS interfaces. The MPLS configuration will be incomplete when the one of the following occurs:

- Only one interface is configured as an MPLS interface.
- MPLS is configured differently on each interface, which causes a protocol mismatch.

In either 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 or pseudowires) the data flow between PE2 and PE3 is affected. In this case Cisco MPLS-AM:

- 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, namely:
  - LSP from PE2 to PE3
  - LSP from PE3 to PE2
- Issues Broken LSP Discovered alarms on both LSPs in PE2 and PE3 correlated to the corresponding MPLS Black Hole Found alarm.

Figure 6-1 MPLS Network Example



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. The auto clear function is used. The ANA gateway server periodically reviews the tickets and checks to see if all the alarms under each ticket are cleared or configured as autocleared alarms. If the alarms are configured as autocleared and the gateway correlation timeout has passed, the gateway closes the case. After the MPLS Black hole alarm is cleared and after the gateway correlation timeout has passed, the gateway closes the ticket because all the alarms correlated to MPLS black hole are broken LSPs, and broken LSP alarms are configured as auto cleared.

BGP Fault Management

Cisco MPLS-AM monitors BGP neighbors and allows you to view correlation and impact analysis information. If BGP connectivity is lost to a device in an IP/MPLS VPN network, the resulting BGP connection loss causes VPN sites to lose connectivity.

The ANA 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 if a loss of connectivity occurs. The Cisco MPLS-AM identifies the faults that affect the BGP connection and reports them as the root cause for the BGP Neighbor Loss alarm.

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

TE Tunnels Fault Management

For TE tunnels, Cisco MPLS-AM supports the MPLS-TE Tunnel Down and MPLS-TE Tunnel Up alarms. When a TE tunnel operational status changes to down and the tunnel is not flapping, a MPLS-TE Tunnel Down alarm is generated. Cisco MPLS-AM identifies the faults that affect the TE tunnel status, for example, Link Down, and reports them as the root cause for the MPLS-TE Tunnel Down alarm. Multiple up and down alarms generated during a short time interval are suppressed and displayed as a MPLS-TE Tunnel Flapping alarm (according to the specific flapping configuration).

After raising the alarms, Cisco MPLS-AM, provides information to help you better understand the business impact on the overall health of the TE network. The TE tunnel alarms are captured at the unit server and forwarded to the gateway server. The Cisco MPLS-AM business impact analysis modules then provide additional information.

All TE tunnel down, up, and reroute alarms are raised. If tunnel down alarm is caused by a failed element, it is correlated to the corresponding element failure alarm. If a reroute occurs on the tunnel and it fails, the reroute alarm is correlated to the tunnel alarm. TE alarm default severity and clearance behavior include the following:

- The MPLS-TE Tunnel Down alarm default severity is Major.
- A MPLS-TE Tunnel Down alarm is cleared by a MPLS-TE Tunnel Up alarm on the same tunnel.

Pseudowires Fault Management

This section describes pseudowire faults and how to access and collect information about tickets generated by the faults. A Layer 2 Tunnel Down alarm is raised when the pseudowire link goes down, namely, the pseudowire tunnel is reported down from both end devices (based on the status of the tunnel), and the tunnel is not flapping.

Cisco MPLS-AM identifies faults that affect the pseudowire tunnel status, for example, Link Down, and reports them as the root cause for the Layer 2 Tunnel Down alarm. Cisco MPLS-AM traces the LSE path to the edge of the pseudowire and marks the edges of the tunnel as affected. Pseudowire alarm default severity and clearance behavior include the following:

- The Layer 2 Tunnel Down default severity is Major.
- The Layer 2 Tunnel Down alarm is cleared by The Layer 2 Tunnel Up alarm on the same tunnel.