Connectivity Outage Detection

The following topics provide a detailed description of Connection Outage Detection (COD) within Cisco MPLS Assurance Manager 1.0 (Cisco MPLS-AM). The following sections tell you how to create and deploy Service Level Agreement (SLA) probes and how to view and monitor probe status:

- Overview, page 9-1
- Creating and Deploying SLA Probes, page 9-3
- Viewing the Status of Probes, page 9-8
- Monitoring, page 9-9

Overview

The Connectivity Outage Detection functions provides a reliable tool to identify network connectivity outage. The tool is an addition to the basic connectivity faults that are accepted and correlated by the underlying fault system. The outage detection tool places probes in the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) network to reliably detect network connectivity outage.

All probes generated with this tool are IP SLA probes. IP SLA is a portfolio of technologies embedded in most devices that run Cisco IOS software, which allows you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLA uses active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance.

Using IP SLAs, you can measure and provide service level agreements and verify service levels, verify outsourced service level agreements, and understand network performance. IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist administrators with network troubleshooting.

IP SLAs can be accessed using the Cisco IOS command-line interface (CLI) or Simple Network Management Protocol (SNMP) through the Cisco Round-Trip Time Monitor (RTTMON) and SYSLOG Management Information Bases (MIBs).

This section describes three main modules:

- Core Connectivity Outage Detection, page 9-2
- VPN Connectivity Outage Detection, page 9-2
- Attachment Circuit Connectivity Outage Detection, page 9-3
Core Connectivity Outage Detection

The Core connectivity module enables IP SLA Health Monitor Probes on PE devices to monitor the MPLS Core LSP connectivity.

In case of network connectivity outage, the probes issue a fault that gets correlated by the underlying fault system and the Impact Analysis module.

The IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs. This feature is useful for determining network availability or testing network connectivity between Provider Edge (PE) routers in an MPLS VPN. Once configured, the LSP Health Monitor will automatically create and delete IP SLAs LSP ping operations based on network topology.

The LSP Health Monitor feature also allows you to perform multioperation scheduling of IP SLA operations and supports proactive threshold violation monitoring through SNMP trap notifications and syslog messages. The syslog messages are transported as traps.

Note
Health Monitor only works for BGP next-hops which are /32 subnets, so the BGP next hop must have a mask of 255.255.255.255.

VPN Connectivity Outage Detection

The VPN connectivity application enables VRF-aware IP SLA probes on PE devices to test attachment circuits and VPN connectivity. The IP SLAs MPLS VPN Aware feature provides the capability to configure IP SLAs operations for specific MPLS VPNs. This feature is an enhancement to the Cisco IOS IP SLA technology that allows you to understand IP service levels, increase productivity, lower operational costs, and reduce the frequency of network outages within MPLS VPNs. IP SLAs use active monitoring of network performance and can be used for network troubleshooting, network assessment, and health monitoring.

Equal Cost Multipaths (ECMPs) can exist between PEs. VRF-aware IP SLA does not monitor each of the ECMPs, it only monitors one. Also ICMP traffic might be treated differently in different environments. In the case of a VPN proactive connectivity there are two options. The first is to have a VRF aware IP SLA from a VRF on the PE to the other PE. (See Figure 9-1.)

Figure 9-1  VPN Connectivity using VRF aware IP SLA from PE to PE

The second option is to have a VRF aware IP SLA from a VRF on the PE to the remote CE. (See Figure 9-2.)
Attachment Circuit Connectivity Outage Detection

As in the case of VCOD, Attachment Circuit Connectivity Outage Detection (ACCOD) is tested using VRF-aware IP SLA probes on PE devices in the VPN connectivity application. IP SLA and its use in ACCOD is described in more detail in Overview, page 9-1. In the case of an attachment circuit, a proactive connectivity VRF aware IP SLA is used from a VRF on the PE to the CE. (See Figure 9-3.)

Creating and Deploying SLA Probes

This section explains how to set up and deploy probes on a device. The creation and deployment of a probes happens in one operation and cannot be separated. SLA probes include Connectivity Outage Detection (CCOD), VPN Connectivity Detection (VCOD), and Access Circuit Connectivity Outage Detection (ACCOD) probes.

This section contains the following topics:

- High-Level Workflow, page 9-4
- Managing CCOD Probes, page 9-4
- Managing VCOD Probes, page 9-5
Creating and Deploying SLA Probes

Managing ACCOD Probes, page 9-6
Viewing the Status of Probes, page 9-8

High-Level Workflow

The process of deploying SLA probes involves the following steps:

1. Set probe parameters—Set the probe parameters based on the SLA, and/or the users sets parameters (their defaults for all values)
2. Activate—Activate the probe for the relevant network entity or entities (PEs, ACs, AC pairs).
3. Get result—Get the results of the activation.
4. Faults handling—Faults are received in the fault system and get correlated.
5. View activated probes—View the activated probes in the logical view of the device.

Managing CCOD Probes

CCOD probes can be created and deployed (in one operation) or deleted. A list of already created probes are displayed in the IP SLA Health Monitor Probe details dialog.

Creating and Deploying a CCOD Probe

To create a CCOD probe, complete the following steps:

Step 1
From the Monitoring menu, choose Connectivity Outage Detection > CCOD Probe Creation.
The CCOD Probe Creation window appears in the workspace under a new tab that is added to any existing tabs in the view.

Step 2
Set probe parameters:

- **Probe ID**—The probe ID value is entered manually. If a probe with the same value already exists in the device, the probe creation operation would fail.
- **LSP Ping Timeout**—Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
- **Number of Consecutive Failures**—Number of times the probe should check for connectivity after which the specified reactive action should be taken.
- **Ping Frequency**—How often pings should be sent.
- **Secondary Frequency**—Frequency at which the probe would check if connectivity has been established, when loss of connectivity or timeout is detected.
- **MPLS EXP Bit**—Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.
- **PE Creation Scan Interval**—Specifies the time interval (in minutes) during which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.
- **PE Deletion Scan Factor**—Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLA operations for BGP next hop neighbors that are no longer valid.
• **TTL**—Specifies the maximum hop count for an echo request packet of an IP SLA operation.
• **Force-Explicit-Null**—MPLS Exp Bits would be configured only when this flag is set to true.
• **Request Data Size**—Specifies the protocol data size for a request packet of an IP SLA operation.
• **Protocol Type**—Parameters for an IP SLA LSP ping or LSP traceroute operation using the LSP Health Monitor.
• **Violation To Be Monitored**—Specifies the violation upon which the reactive action is to be taken. Examples: loss of connectivity or timeout.
• **Action To Be Taken For Violation**—Reactive action to be taken when the violation is detected. For example to raise a trap.
• **Threshold-type For Violation**—How the probe should react when a violation is detected. Examples: The probe should react over average of N attempts, consecutive occurrences of the fault, react immediately, etc.

**Step 3** (Optional) Validate the probe by checking for errors using the **Validate the Probe** button.
It verifies if the values entered for probe creation are valid and whether the probe would be successfully created in the device.

**Step 4** (Optional) View the associated CLI before the probe is deployed by clicking the **Preview the CLI** button.
This displays the IOS commands that would be executed in the device to create the probe.

**Step 5** To deploy the CCOD probe, click the **Deploy the Probe** button.

**Step 6** The status of the probe can be seen by launching the IP SLA HM probe details dialog.

---

**Deleting CCOD Probes**

To delete a CCOD probe, launch the IP LSA HM Probe Details dialog. Select the probe to be deleted and click the **Deactivate** button.

**Managing VCOD Probes**

VCOD probes can be created and deployed (in one operation) or deleted. List of already created probes are displayed in IP SLA Probe details dialog.

**Creating and Deploying a VCOD Probe**

To create a VCOD probe, complete the following steps:

**Step 1** From the Monitoring menu, choose **Connectivity Outage Detection > VCOD Probe Creation**.
The VCOD Probe Creation window appears in the workspace under a new tab that is added to any existing tabs in the view.

**Step 2** In the **Threshold-type For Violation** drop-down list, choose how the probe should react when a violation is detected.
Examples: You can choose to let the probe react over an average of N attempts, on consecutive occurrences of the fault, immediately, etc.
Creating and Deploying SLA Probes

Step 3  Choose from the following options:

- **Short Reach (PE-PE)**—Use in the case of a VRF aware IP SLA from a VRF on a PE to another PE. 
  (See Figure 9-1.)

- **Long Reach (PE-CE)**—Use in the case of a VRF aware IP SLA from a VRF on the PE to the remote CE. (See Figure 9-2.)

- **Load Balance**—This flag only applies to Short Reach as the probe can only be created on the PE. When this flag is set, the PE which has the least number of probes configured in the VPN would be chosen for IP SLA probe creation. This option creates the probe on the device, which frees up more memory.

Step 4  If you chose Short Reach in Step 3, complete the following steps. If you choose Long Reach, continue with Step 5.

a. When selecting **Short Reach**, a list of available PEs in the VPN is displayed in the Probe Source list. Depending on the selected source PE, possible Probe Destination PE interfaces will be displayed.

b. Choose one of the possible destination PE interfaces.

c. (Optional) Validate the probe by checking for errors using the **Validate the Probe** button. It verifies if the values entered for probe creation are valid and whether the probe would be successfully created in the device.

d. (Optional) View the associated CLI before the probe is deployed by clicking the **Preview the CLI** button. This displays the IOS commands that would be executed in the device to create the probe.

e. To deploy the VCOD probe, click the **Deploy the Probe** button.

f. The status of the probe can be seen by launching the IP SLA probe details dialog.

Step 5  If you chose Long Reach in Step 3, complete the following steps:

a. When selecting **Long Reach**, a list of available PEs in the VPN is displayed in the Probe Source list. Depending on the selected source PE, possible Probe Destination CE interfaces will be displayed.

b. Choose one of the possible destination CE interfaces.

c. (Optional) Validate the probe by checking for errors using the **Validate the Probe** button. It verifies if the values entered for probe creation are valid and whether the probe would be successfully created in the device.

d. (Optional) View the associated CLI before the probe is deployed by clicking the **Preview the CLI** button. This displays the IOS commands that would be executed in the device to create the probe.

e. To deploy the VCOD probe, click the **Deploy the Probe** button.

f. The status of the probe can be seen by launching the IP SLA probe details dialog.

Deleting VCOD Probes

To delete a VCOD probe, launch the IP LSA Probe Details dialog. Select the probe to be deleted and click the **Deactivate** button.

Managing ACCOD Probes

ACCOD probes can be created and deployed (in one operation) or deleted.
Creating and Deploying ACCOD Probes

To create a ACCOD probe, complete the following steps:

**Step 1**  
From the Monitoring menu, choose **Connectivity Outage Detection > ACCOD Probe Creation.**  
The ACCOD Probe Creation window appears in the workspace under a new tab that is added to any existing tabs in the view.

**Step 2**  
Set the probe parameters:

- **Probe ID**—The probe ID value is entered manually. If a probe with the same value already exists in the device, the probe creation operation would fail.
- **RTT Response Timeout**—Specifies the amount of time the IP SLA operation waits for a response from its request packet.
- **Number of Consecutive Failures**—Number of times the probe should check for connectivity after which the specified reactive action should be taken.
- **Ping Frequency**—How often pings should be sent.
- **DSCP Values**—Differentiated service code point values.
- **Request Data Size**—Specifies the protocol data size for a request packet of an IP SLA operation.
- **Probe Lifetime**—Specifies the lifetime of the IP SLA probe.
- **Protocol Type**—Parameters for an IP SLA LSP ping or LSP traceroute operation using the LSP Health Monitor.
- **Violation To Be Monitored**—Specifies the violation upon which the reactive action is to be taken. *(loss of connectivity or timeout).*
- **Action To Be Taken For Violation**—Reactive action to be taken when the violation is detected. For example to raise a trap.
- **Threshold-type For Violation**—How the probe should react when a violation is detected.  
Examples: The probe should react over average of N attempts, consecutive occurrences of the fault, react immediately, etc.

**Step 3**  
*(Optional)* Validate the probe by checking for errors using the **Validate the Probe** button.  
It verifies if the values entered for probe creation are valid and whether the probe would be successfully created in the device.

**Step 4**  
*(Optional)* View the associated CLI before the probe is deployed by clicking the **Preview the CLI** button.  
This displays the IOS commands that would be executed in the device to create the probe.

**Step 5**  
To deploy the ACCOD probe, click the **Deploy the Probe** button.

**Step 6**  
The status of the probe can be seen by launching the IP SLA probe details dialog.

Deleting ACCOD Probes

To delete an ACCOD probe, launch the IP LSA Probe Details dialog. Select the probe to be deleted and click the **Deactivate** button.
Viewing the Status of Probes

To view the status of probes that have been deployed, use one of the following tools from the Monitoring menu:

- IP SLA Probe Info, page 9-8
- Health Monitor Probe Info, page 9-9

IP SLA Probe Info

The IP SLA Probe Info option is used to view the status of VCOD and ACCOD probes. The following two operations are available:

- Showing the Operational Status of a VCOD or ACCOD Probe, page 9-8
- Deactivating a VCOD or ACCOD Probe, page 9-8

Showing the Operational Status of a VCOD or ACCOD Probe

To show the operational status of a VCOD or ACCOD probe, complete the following steps:

Step 1 From the Monitoring menu, choose Connectivity Outage Detection > IP SLA Probe Details.
Step 2 In the device list, select the device in question.
Step 3 In the IP SLA probe list, select an associated IP SLA probe.
Step 4 Click the Operational Status button.
The Operational Status window opens.
Step 5 Review the operational status details to determine the status of the selected probe.
Step 6 Close the Operational Status window.

Deactivating a VCOD or ACCOD Probe

To deactivate a VCOD or ACCOD probe, complete the following steps:

Step 1 From the Monitoring menu, choose Connectivity Outage Detection > IP SLA Probe Info.
Step 2 In the Probe Details window, select a VCOD or ACCOD probe.
The properties of the selected probe are shown in the CSV view under the Properties tab. These values are configured at the time of probe creation.
- Property—Property configured for the probe selected in the workspace
- Value—Value of the property
Step 3 Click the Deactivate button.
The probe is immediately removed.
Health Monitor Probe Info

The Health Monitor Probe Info option is used to view the status of CCOD probes. This is done because these two types of probes are structured in the same way. In the Health Monitor Probe viewer, only the Deactivate Probe operation is available.

Deactivating a CCOD Probe

To deactivate a CCOD probe, complete the following steps:

1. From the Monitoring menu, choose Connectivity Outage Detection > IP SLA HM Probe Info.
2. In the Probe Details window, select a CCOD probe.
   - The properties of the selected probe are those that have been configured and are shown in the CSV view under the Properties tab.
   - Property—Property configured for the probe selected in the workspace.
   - Value—Value of the property.
3. Click the Deactivate button.
   - A Confirmation window appears.
4. Click OK to confirm that the IP SLA probe(s) should be removed.
   - The probe is removed.

Monitoring

This section discusses alarms and fault correlation techniques used to monitor and assess the status of COD probes. Go to the Troubleshooting perspective to access these features.

Alarms

In ANA, an alarm represents a scenario which involves a fault occurring in the network or management system. Alarms represent the complete fault lifecycle, from the time that the alarm is opened (when the fault is first detected) until it is closed and acknowledged. Under connectivity outage detection, each alarm is derived from a specific trap sent from a device, meaning, there is a one-to-one relationship between a trap and one of the following alarms.

There are three types of IP SLA alarms:

- IP SLA A/C—Raised in the case of an access circuit failure.
- IP SLA L3 MPLS VPN—Raised in the case of a VPN outage.
- IP SLA LSP—Raised in the case of a core (PE-PE) outage.
Fault Correlation

ANA can be used for analyzing and managing faults through fault detection, isolation, and correlation. After a fault is identified, the system uses the autodiscovered virtual network model to perform fault inspection and correlation to determine the root cause of the fault and, if applicable, to perform service impact analysis.

There are three types of IP SLA alarms, each of which can be associated with a potential root cause. The behavior is as follows:

- All IP SLA alarms with a root cause correlate to the same trouble ticket based on the existence of a common root cause.
- All IP SLA alarms without a root cause correlate based on a time.

Viewing Deployed Probe Alarms

To view any alarms that might be associated with a deployed probe, complete the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Window menu, choose <strong>Open Perspective &gt; Troubleshooting</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the navigation area, select the <strong>Object</strong> tab</td>
</tr>
</tbody>
</table>
| Step 3 | Double-click **Tickets**.  
A list of tickets appears. |
| Step 4 | Select the desired COD alarm. |
| Step 5 | For correlation details, view the Correlation pane at the bottom part of the workspace. |