



EFT REVIEW DRAFT – CISCO CONFIDENTIAL

# Configuring Cisco IOS IP SLAs LSP Health Monitor Operations

---

**First Published: February 27, 2007**  
**Last Updated: February 14, 2011**

This module describes how to configure a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor with LSP Discovery feature. LSP health monitors enable you to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides automated end-to-end verification in the control plane and data plane for all LSPs between the participating Provider Edge (PE) routers. This end-to-end (PE-to-PE router) approach ensures that LSP connectivity is verified along the paths that customer traffic is sent. Consequently, customer-impacting network connectivity issues that occur within the MPLS core will be detected by the LSP Health Monitor. Once configured, the LSP Health Monitor will automatically create and delete IP SLAs LSP ping or LSP traceroute operations based on network topology.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for LSP Health Monitor Operations](#)” section on page 39.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for LSP Health Monitor Operations, page 2](#)
- [Restrictions for LSP Health Monitor Operations, page 2](#)
- [Information About LSP Health Monitor Operations, page 2](#)
- [How to Configure LSP Health Monitor Operations, page 11](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007-2010 Cisco Systems, Inc. All rights reserved.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

- [Configuration Examples for the LSP Health Monitor, page 28](#)
- [Additional References, page 37](#)
- [Feature Information for LSP Health Monitor Operations, page 39](#)

## Prerequisites for LSP Health Monitor Operations

- The participating PE routers of an LSP Health Monitor operation must support the MPLS LSP ping feature. It is recommended that the Provider (P) routers also support the MPLS LSP Ping feature in order to obtain complete error reporting and diagnostics information.
- Ensure that the source PE router has enough memory to support the desired LSP Health Monitor functionality. Enabling the LSP discovery option can potentially have a significant impact on router memory. If there is not enough memory available during the LSP discovery process, the process will gracefully terminate and an error message will be displayed.

**Note**

The destination PE routers of an LSP Health Monitor operation do not require the IP SLAs Responder to be enabled.

## Restrictions for LSP Health Monitor Operations

- Once an LSP Health Monitor operation is started, its configuration parameters should not be changed until the operation has ended. Changing the configuration parameters while the operation is actively running could cause delays in obtaining network connectivity statistics.

## Information About LSP Health Monitor Operations

- [Benefits of the LSP Health Monitor, page 2](#)
- [How the LSP Health Monitor Works, page 3](#)
- [Discovery of Neighboring PE Routers, page 4](#)
- [The LSP Discovery Process, page 5](#)
- [LSP Discovery Groups, page 7](#)
- [IP SLAs LSP Ping and LSP Traceroute Operations, page 8](#)
- [IP SLAs VCCV Operation, page 8](#)
- [Proactive Threshold Monitoring for the LSP Health Monitor, page 9](#)
- [Multioperation Scheduling for the LSP Health Monitor, page 10](#)

## Benefits of the LSP Health Monitor

- End-to-end LSP connectivity measurements across equal-cost multipaths for determining network availability or testing network connectivity in MPLS networks
- Proactive threshold monitoring through SNMP trap notifications and syslog messages

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

- Reduced network troubleshooting time for MPLS networks
- Scalable network error detection using fast retry capability
- Creation and deletion of IP SLAs operations based on network topology
- Discovery of Border Gateway Protocol (BGP) next hop neighbors based on local VRF routing and forwarding instances (VRFs) and global routing tables
- Multioperation scheduling of IP SLAs operations
- Pseudo-wire connectivity testing between MPLS network edges, with threshold violations and scalable operation scheduling
- Monitoring and SNMP trap alerts for round-trip time (RTT) threshold violations, connection loss, and command response timeouts

## How the LSP Health Monitor Works

The LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs. The general process for how the LSP Health Monitor works is as follows:

1. The user configures an LSP Health Monitor operation and the BGP next hop neighbor discovery process is enabled.

Configuring an LSP Health Monitor operation is similar to configuring a standard IP SLAs operation. To illustrate, all operation parameters for an LSP Health Monitor operation are configured after an identification number for the operation is specified. However, unlike standard IP SLAs operations, these configured parameters are then used as the base configuration for the individual IP SLAs LSP ping and LSP traceroute operations that will be created by the LSP Health Monitor. The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE router. To prevent unnecessary router performance issues, careful consideration should be taken when configuring the operational and scheduling parameters of an LSP Health Monitor operation.

When the BGP next hop neighbor discovery process is enabled, a database of BGP next hop neighbors in use by any VRF associated with the source PE router is generated based on information from the local VRF and global routing tables. For more information about the BGP next hop neighbor discovery process, see the [“Discovery of Neighboring PE Routers”](#) section on page 4.



**Note** By default, only a single path between the source and destination PE routers is discovered. If the LSP discovery option is enabled, the equal-cost multipaths between the source and destination PE routers are discovered. For more information on how the LSP discovery process works, see [“The LSP Discovery Process”](#) section on page 5.

2. The user configures proactive threshold monitoring parameters for the LSP Health Monitor operation. For more information about proactive threshold monitoring, see the [“Proactive Threshold Monitoring for the LSP Health Monitor”](#) section on page 9.

Depending on the proactive threshold monitoring configuration options chosen, SNMP trap notifications or syslog messages are generated as threshold violations are met.

3. The user configures multioperation scheduling parameters for the LSP Health Monitor operation. For more information about multioperation scheduling, see the [“Multioperation Scheduling for the LSP Health Monitor”](#) section on page 10.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created (based on parameters configured in Step 1) for each applicable PE (BGP next hop) neighbor. The IP SLAs operations will measure network connectivity between the source PE router and the discovered destination PE router. The start time and frequency of each measurement is based on the multioperation scheduling parameters defined by the user.

**Addition and Deletion of IP SLAs Operations**

The LSP Health Monitor receives periodic notifications about BGP next hop neighbors that have been added to or removed from a particular VPN. This information is stored in a queue maintained by the LSP Health Monitor. Based on the information in the queue and user-specified time intervals, new IP SLAs operations are automatically created for newly discovered PE routers and existing IP SLAs operations are automatically deleted for any PE routers that are no longer valid. The automatic deletion of operations can be disabled. However, disabling this function is not recommended because these operations would then need to be deleted manually.

If the LSP discovery option is enabled, creation of LSP discovery groups for newly discovered BGP next hop neighbors will follow the same process as described in the [“The LSP Discovery Process”](#) section on page 5. If a BGP next hop neighbor is removed from a particular VPN, all the corresponding LSP discovery groups and their associated individual IP SLAs operations and statistics are removed from the LSP discovery group database.

**Access Lists for Filtering BGP Next Hop Neighbors**

Standard IP access lists can be configured to restrict the number of IP SLAs operations that are automatically created by the LSP Health Monitor. When the IP SLAs access list parameter is configured, the list of BGP next hop neighbors discovered by the LSP Health Monitor is filtered based on the conditions defined by the associated standard IP access list. In other words, the LSP Health Monitor will automatically create IP SLAs operations only for those BGP next hop neighbors with source addresses that satisfy the criteria permitted by the standard IP access list.

**Unique Identifier for Each Automatically Created IP SLAs Operation**

The IP SLAs operations automatically created by the LSP Health Monitor are uniquely identified by their owner field. The owner field of an operation is generated using all the parameters that can be configured for that particular operation. If the length of the owner field is longer than 255 characters, it will be truncated.

## Discovery of Neighboring PE Routers

A BGP next hop neighbor discovery process is used to find the BGP next hop neighbors in use by any VRF associated with the source PE router. In most cases, these neighbors will be PE routers.

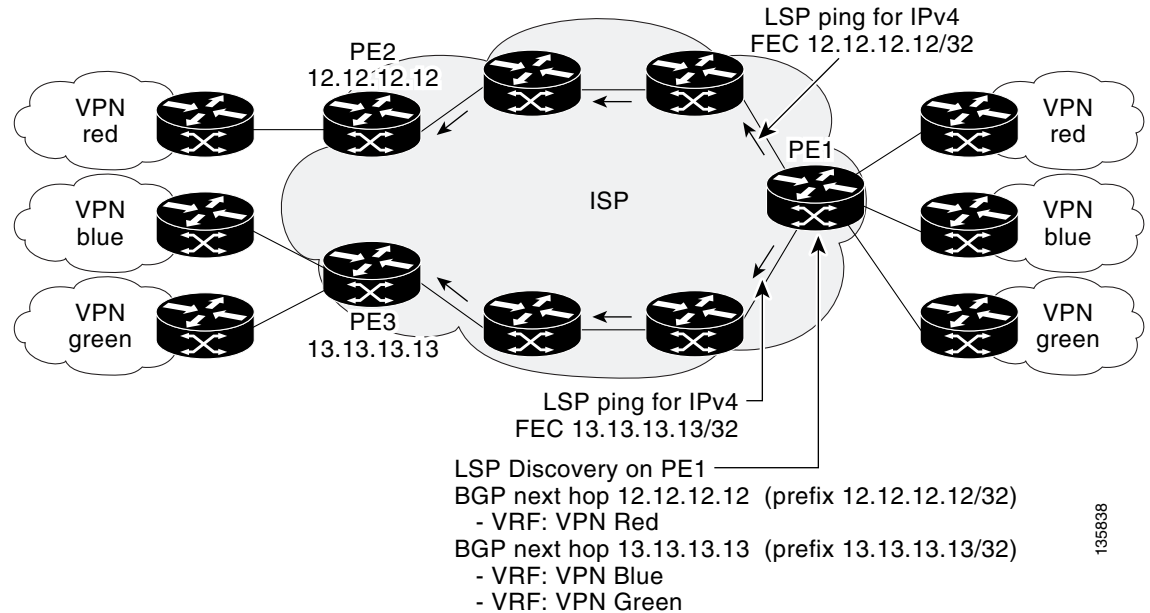
When the BGP next hop neighbor discovery process is enabled, a database of BGP next hop neighbors in use by any VRF associated with the source PE router is generated based on information from the local VRF and global routing tables. As routing updates are received, new BGP next hop neighbors are added to and deleted from the database immediately.

**Figure 1** shows how the BGP next hop neighbor discovery process works for a simple VPN scenario for an Internet service provider (ISP). In this example, there are three VPNs associated with router PE1: red, blue, and green. From the perspective of router PE1, these VPNs are reachable remotely through BGP next hop neighbors PE2 (router ID: 12.12.12.12) and PE3 (router ID: 13.13.13.13). When the BGP next hop neighbor discovery process is enabled on router PE1, a database is generated based on the local VRF and global routing tables. The database in this example contains two BGP next hop router entries: PE2 12.12.12.12 and PE3 13.13.13.13. The routing entries are maintained per next hop router to distinguish

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

which next hop routers belong within which particular VRF. For each next hop router entry, the IPv4 Forward Equivalence Class (FEC) of the BGP next hop router in the global routing table is provided so that it can be used by the MPLS LSP ping operation.

**Figure 1 BGP Next Hop Neighbor Discovery for a Simple VPN**



## The LSP Discovery Process

The LSP discovery option of an LSP Health Monitor operation provides the capability to discover the equal-cost multipaths for carrying MPLS traffic between the source and destination PE routers. Network connectivity measurements can then be performed for each of the paths that were discovered.

The general process for LSP discovery is as follows:

1. BGP next hop neighbors are discovered using the BGP next hop neighbor discovery process. For more information about the BGP next hop neighbor discovery process, see the [“Discovery of Neighboring PE Routers”](#) section on page 4.

Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created for each applicable PE (BGP next hop) neighbor. Only a single path to each applicable PE neighbor is discovered during this initial step of the LSP discovery process. For each next hop neighbor, the LSP Health Monitor creates an LSP discovery group (that initially consists of only the one discovered path) and assigns the group with a unique identification number. For more information about LSP discovery groups, see the [“LSP Discovery Groups”](#) section on page 7.

2. An LSP discovery request is sent by the LSP Health Monitor to the LSP discovery subsystem for each applicable BGP next hop neighbor. For each next hop neighbor in which an appropriate response is received, MPLS echo requests are sent one-by-one from the source PE router to discover the equal-cost multipaths. The parameters that uniquely identify each equal-cost multipath (127/8 destination IP address [LSP selector] and the PE outgoing interface) are added to the associated LSP discovery database.

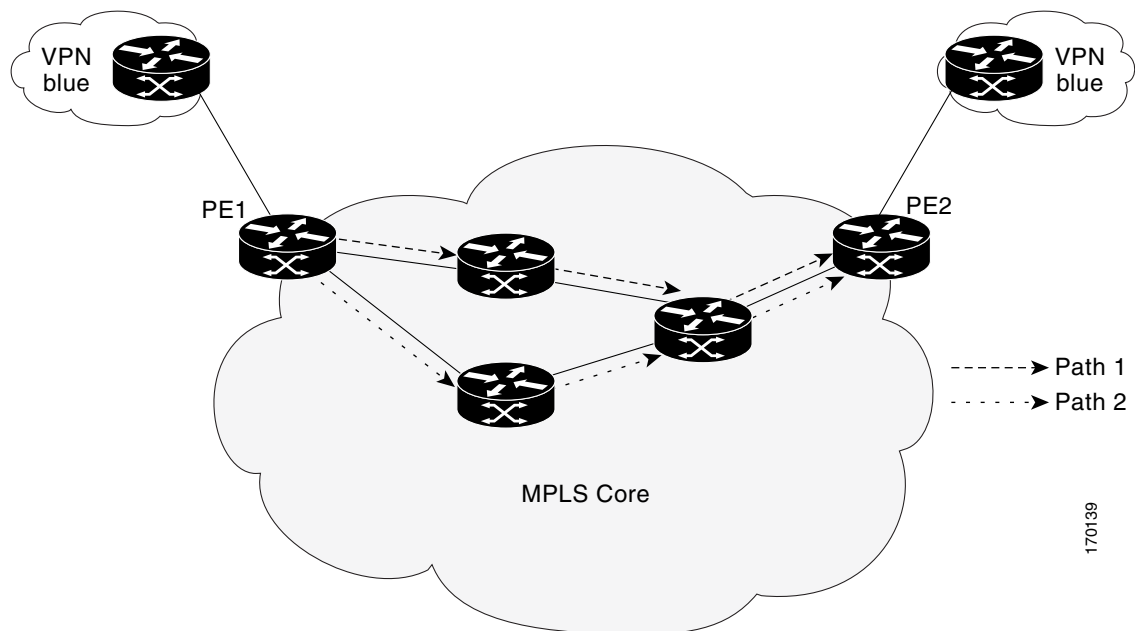
**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

**Note** For a given LSP Health Monitor operation, the user can define the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery.

- Each individual IP SLAs operation (created for each applicable PE neighbor) uses an IP SLAs LSP ping superoperation to measure network connectivity across all equal-cost multipaths between the source PE router and discovered destination PE router. The IP SLAs superoperation operates by sending an LSP ping packet to the destination PE router and adjusting the LSP ping 127/8 LSP selector IP address for each discovered equal-cost multipath. For example, assume that there are three equal-cost multipaths to a destination PE router and the identified LSP selector IP addresses are 127.0.0.1, 127.0.0.5, and 127.0.0.6. The IP SLAs superoperation would sequentially send three LSP ping packets using the identified LSP selector IP addresses for directing the superoperation across the three paths. This technique ensures that there is only a single IP SLAs LSP ping operation for each source and destination PE router pair, and significantly reduces the number of active LSP ping operations sent by the source PE router.

Figure 2 illustrates a simple VPN scenario. This network consists of a core MPLS VPN with two PE routers (router PE1 and router PE2) belonging to the VRF named VPN blue. Suppose router PE1 is the source PE router for an LSP Health Monitor operation with the LSP discovery option enabled and that router PE2 is discovered by the BGP discovery process as a BGP next hop neighbor to router PE1. If path 1 and path 2 are equal-cost multipaths between router PE1 to router PE2, then the LSP discovery process would create an LSP discovery group consisting of path 1 and path 2. An IP SLAs LSP ping superoperation would also be created to monitor network availability across each path.

**Figure 2** LSP Discovery for a Simple VPN



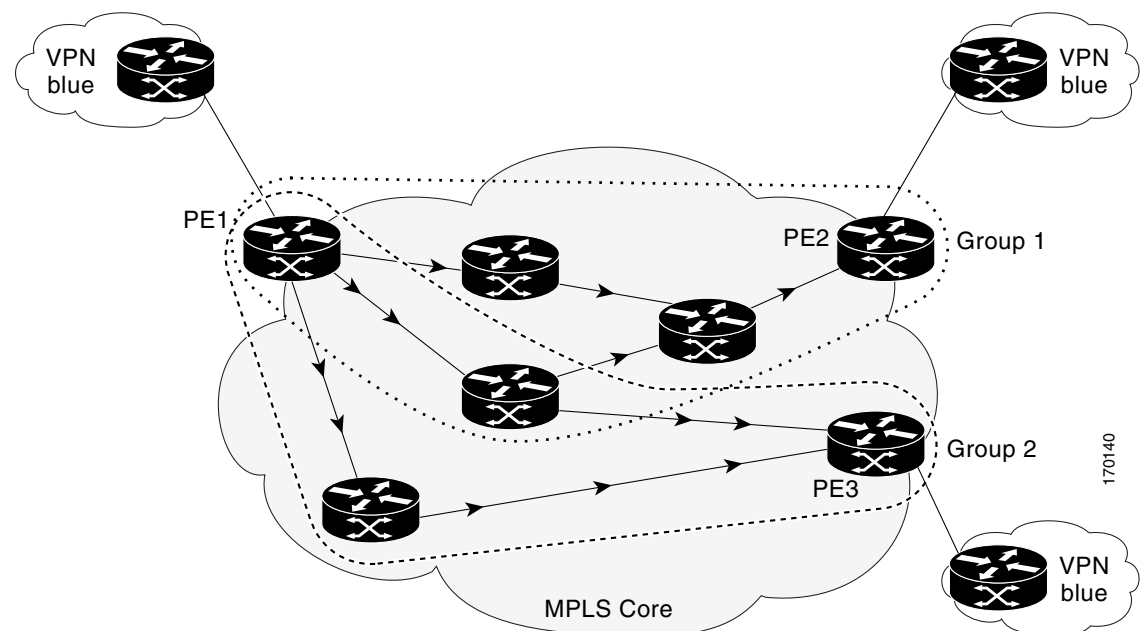
170139

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

## LSP Discovery Groups

A single LSP Health Monitor operation can be comprised of several LSP discovery groups depending on the number of BGP next hop neighbors discovered by the BGP next hop neighbor discovery process. Each LSP discovery group corresponds to one BGP next hop neighbor and is assigned a unique identification number (starting with the number 1). [Figure 3](#) illustrates a simple VPN scenario. This network consists of a core MPLS VPN with three PE routers (router PE1, PE2, and PE3) belonging to the VRF named VPN blue. Suppose router PE1 is the source PE router for an LSP Health Monitor operation with the LSP discovery option enabled and that router PE2 and PE3 are discovered by the BGP discovery process as BGP next hop neighbors to router PE1. LSP discovery group 1 is created for the equal-cost multipaths between router PE1 to router PE2 and LSP discovery group 2 is created for the equal-cost multipaths between router PE1 to router PE3.

**Figure 3** LSP Discovery Groups for a Simple VPN



Once the LSP Health Monitor operation is started, a single IP SLAs operation is automatically created for each applicable PE (BGP next hop) neighbor. Each IP SLAs operation (created for each applicable PE neighbor) uses an IP SLAs LSP ping superoperation to measure network connectivity across all equal-cost multipaths between the source PE router and discovered destination PE router. Each LSP ping superoperation corresponds to a single LSP discovery group.

The LSP ping superoperation operates by sending an LSP ping packet to the destination PE router and adjusting the LSP ping 127/8 LSP selector IP address for each discovered equal-cost multipath. The network connectivity statistics collected by each equal-cost multipath is aggregated and stored in one-hour increments (data can be collected for a maximum of two hours). Results are stored as group averages representative of all the equal-cost multipaths within the LSP discovery group for a given one-hour increment.

Each equal-cost multipath discovered between the source PE router and a BGP next hop neighbor is uniquely identified with the following parameters:

- 127/8 destination IP address (LSP selector) within the local host IP address range



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

- PE outgoing interface

The database for an LSP discovery group is updated if any of the following events occur:

- The corresponding LSP ping superoperation sends an LSP ping packet.
- An active equal-cost multipath is added to or deleted from the LSP discovery group.
- The user enters the Cisco IOS command to delete all the aggregated statistical data for a particular LSP discovery group.

## IP SLAs LSP Ping and LSP Traceroute Operations

This feature introduces support for the IP SLAs LSP ping and IP SLAs LSP traceroute operations. These operations are useful for troubleshooting network connectivity issues and determining network availability in an MPLS VPN. When using the LSP Health Monitor, IP SLAs LSP ping and LSP traceroute operations are automatically created to measure network connectivity between the source PE router and the discovered destination PE routers. Individual IP SLAs LSP ping and LSP traceroute operations can also be manually configured. Manual configuration of these operations can be useful for troubleshooting a connectivity issue.

The IP SLAs LSP ping and IP SLAs LSP traceroute operations are based on the same infrastructure used by the MPLS LSP Ping and MPLS LSP Traceroute features, respectively, for sending and receiving echo reply and request packets to test LSPs.

The LSP discovery option does not support IP SLAs traceroute operations.

## IP SLAs VCCV Operation

The IP SLAs VCCV operation supports Virtual Circuit Connectivity Verification (VCCV) for Pseudo-Wire Emulation Edge-to-Edge (PWE3) services across MPLS networks. The IP SLAs VCCV operation type is based on the **ping mpls pseudowire** command, which checks MPLS LSP connectivity across an Any Transport over MPLS (AToM) virtual circuit (VC) by sending a series of pseudo-wire ping operations to the specified destination PE router.

When MPLS LSP connectivity checking is performed through an IP SLAs VCCV operation (rather than through the **ping mpls** command with the **pseudowire** keyword), you can use the IP SLA proactive threshold monitoring and multioperation scheduling capabilities:

- You can configure an IP SLAs VCCV operation to perform proactive monitoring of PWE3 services and detection of faults in those services. An IP SLAs VCCV operation can send out a Simple Network Management Protocol (SNMP) trap if round-trip time (RTT) thresholds are violated, if the connection is lost, or if a command response timeout occurs. In addition, RTT data is available to be reported as statistics. For more information, see the [“Proactive Threshold Monitoring for the LSP Health Monitor”](#) section on page 9.
- Through the use of the **ip sla schedule** command, you can schedule an IP SLAs VCCV operation to periodically perform VCCV for PWE3 services. For more information, see the [“Multioperation Scheduling for the LSP Health Monitor”](#) section on page 10.

The LSP discovery option does not support the IP SLAs VCCV operation.



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

## Proactive Threshold Monitoring for the LSP Health Monitor

Proactive threshold monitoring support for the LSP Health Monitor feature provides the capability for triggering SNMP trap notifications and syslog messages when user-defined reaction conditions (such as a connection loss or timeout) are met. Configuring threshold monitoring for an LSP Health Monitor operation is similar to configuring threshold monitoring for a standard IP SLAs operation.

### LSP Discovery Option Enabled

If the LSP discovery option for an LSP Health Monitor operation is enabled, SNMP trap notifications can be generated when one of the following events occurs:

- LSP discovery for a particular BGP next hop neighbor fails.
- Operational status of an LSP discovery group changes.

Possible reasons for which LSP discovery can fail for a particular BGP next hop neighbor are as follows:

- Expiration of time allowed for a BGP next hop neighbor to respond to an LSP discovery request.
- Return code is “Broken” or “Unexplorable” for all paths leading to the BGP next hop neighbor.

[Table 1](#) describes the conditions for which the operational status of an LSP discovery group can change. Whenever an individual IP SLAs LSP ping operation of an LSP discovery group is executed, a return code is generated. Depending on the value of the return code and the current status of the LSP discovery group, the group status can change.

**Table 1**      **Conditions for Which an LSP Discovery Group Status Changes**

Individual IP SLAs Operation Return Code	Current Group Status = UP	Current Group Status = PARTIAL	Current Group Status = DOWN
OK	No group status change.	If return codes for all paths in the group are OK, then the group status changes to UP.	Group status changes to PARTIAL.
Broken or Unexplorable	Group status changes to PARTIAL.	If return codes for all paths in the group are Broken or Unexplorable, then the group status changes to DOWN.	No group status change.

The return code for an individual IP SLAs LSP ping operation can be one of the following:

- OK—Indicates that the LSP is working properly. The customer VPN traffic will be sent across this path.
- Broken—Indicates that the LSP is broken. Customer VPN traffic will not be sent across this path and may be discarded.
- Unexplorable—Indicates that not all the paths to this PE neighbor have been discovered. This may be due to a disruption along the LSP or because the number of 127/8 IP addresses used for LSP selection has been exhausted.

The status of an LSP discovery group can be one of the following:

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

- UNKNOWN—Indicates that group status has not yet been determined and that the paths belonging to the group are in the process of being tested for the first time. Once this initial test is complete, the group status will change to UP, PARTIAL, or DOWN.
- UP—Indicates that all the paths within the group are active and no operation failures have been detected.
- PARTIAL—Indicates that an operation failure has been detected for one or more, but not all, of the paths within the group.
- DOWN—Indicates that an operation failure has been detected for all the paths within the group.

**Secondary Frequency Option**

With the introduction of the LSP Health Monitor feature, a new threshold monitoring parameter has been added that allows you to specify a secondary frequency. If the secondary frequency option is configured and a failure (such as a connection loss or timeout) is detected for a particular path, the frequency at which the path is remeasured will increase to the secondary frequency value (testing at a faster rate). When the configured reaction condition is met (such as N consecutive connection losses or N consecutive timeouts), an SNMP trap and syslog message can be sent and the measurement frequency will return to its original frequency value.

## Multioperation Scheduling for the LSP Health Monitor

Multioperation scheduling support for the LSP Health Monitor feature provides the capability to easily schedule the automatically created IP SLAs operations (for a given LSP Health Monitor operation) to begin at intervals equally distributed over a specified duration of time (schedule period) and to restart at a specified frequency. Multioperation scheduling is particularly useful in cases where the LSP Health Monitor is enabled on a source PE router that has a large number of PE neighbors and, therefore, a large number of IP SLAs operations running at the same time.

Newly created IP SLAs operations (for newly discovered BGP next hop neighbors) are added to the same schedule period as the operations that are currently running. To prevent too many operations from starting at the same time, the multioperation scheduling feature will schedule the operations to begin at random intervals uniformly distributed over the schedule period.

Configuring a multioperation schedule for the LSP Health Monitor is similar to configuring a standard multioperation schedule for a group of individual IP SLAs operations.

**LSP Discovery Option Enabled**

When a multioperation schedule for an LSP Health Monitor operation with LSP discovery is started, the BGP next hop neighbors are discovered, and network connectivity to each applicable neighbor is monitored using only a single LSP. In other words, initially, network connectivity between the source PE router and discovered destination PE router is measured across only a single path. This initial condition is the same as if an LSP Health Monitor operation was performed without LSP discovery.

Specific information about the IP SLAs LSP ping operations that are created for newly discovered equal-cost paths during the succeeding iterations of the LSP discovery process are stored in the LSP discovery group database. These newly created IP SLAs LSP ping operations will start collecting data at the next iteration of network connectivity measurements for their associated LSP discovery group.

The start times for the individual IP SLAs LSP ping operations for each LSP discovery group is based on the number of LSP discovery groups and the schedule period of the multioperation schedule. For example, if three LSP discovery groups (Group 1, Group 2, and Group 3) are scheduled to run over a period of 60 seconds, the first LSP ping operation of Group 1 will start at 0 seconds, the first LSP ping operation of Group 2 will start at 20 seconds, and the first LSP ping operation of Group 3 will start at

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

40 seconds. The remaining individual IP SLAs LSP ping operations for each LSP discovery group will run sequentially after completion of the first LSP ping operation. For each LSP discovery group, only one LSP ping operation runs at a time.

## How to Configure LSP Health Monitor Operations

- [Configuring an LSP Health Monitor Operation, page 11](#) (required)
- [Scheduling LSP Health Monitor Operations, page 18](#) (required)
- [Manually Configuring and Scheduling an IP SLAs LSP Ping or LSP Traceroute Operation, page 20](#) (optional)
- [Manually Configuring and Scheduling an IP SLAs VCCV Operation](#) (optional)
- [Verifying and Troubleshooting LSP Health Monitor Operations, page 26](#) (optional)

## Configuring an LSP Health Monitor Operation

Perform only one of the following tasks:

- [Configuring an LSP Health Monitor Operation Without LSP Discovery on a PE Router, page 11](#)
- [Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Router, page 15](#)

## Configuring an LSP Health Monitor Operation Without LSP Discovery on a PE Router

### Restrictions

- If the LSP discovery option is disabled, only a single path between the source PE router and each BGP next hop neighbor is discovered.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval** *seconds*
5. **auto ip sla mpls-lsp-monitor** *operation-number*
6. **type echo** [*ipsla-vrf-all* | *vrf vpn-name*]  
or  
**type pathEcho** [*ipsla-vrf-all* | *vrf vpn-name*]
7. **access-list** *access-list-number*
8. **scan-interval** *minutes*
9. **delete-scan-factor** *factor*
10. **force-explicit-null**
11. **exp** *exp-bits*
12. **lsp-selector** *ip-address*

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

13. **reply-dsep-bits** *dscp-value*
14. **reply-mode** {*ipv4* | *router-alert*}
15. **request-data-size** *bytes*
16. **secondary-frequency** {*both* | *connection-loss* | *timeout*} *frequency*
17. **tag** *text*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **tfl** *time-to-live*
21. **exit**
22. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {*connectionLoss* | *timeout*} [*action-type option*] [*threshold-type* {*consecutive* [*occurrences*] | *immediate* | *never*}]
23. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>mpls discovery vpn next-hop</b>  <b>Example:</b> Router(config)# mpls discovery vpn next-hop	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process.  <b>Note</b> This command is automatically enabled when the <b>auto ip sla mpls-lsp-monitor</b> command is entered.
<b>Step 4</b>	<b>mpls discovery vpn interval seconds</b>  <b>Example:</b> Router(config)# mpls discovery vpn interval 120	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
<b>Step 5</b>	<b>auto ip sla mpls-lsp-monitor operation-number</b>  <b>Example:</b> Router(config)# auto ip sla mpls-lsp-monitor 1	Begins configuration for an LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.  <b>Note</b> Entering this command automatically enables the <b>mpls discovery vpn next-hop</b> command.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 6</b>	<pre>type echo [ipsla-vrf-all   vrf vpn-name] or type pathEcho [ipsla-vrf-all   vrf vpn-name]</pre> <p><b>Example:</b> Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all or</p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all</p>	<p>Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.</p> <p>or</p> <p>Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP traceroute operation using the LSP Health Monitor.</p>
<b>Step 7</b>	<pre>access-list access-list-number</pre> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-params)# access-list 10</p>	(Optional) Specifies the access list to apply to an LSP Health Monitor operation.
<b>Step 8</b>	<pre>scan-interval minutes</pre> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-params)# scan-interval 5</p>	(Optional) Sets the timer for the IP SLAs LSP Health Monitor database.
<b>Step 9</b>	<pre>delete-scan-factor factor</pre> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-params)# delete-scan-factor 2</p>	<p>(Optional) Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.</p> <ul style="list-style-type: none"> <li>• The default scan factor is 1. Each time the LSP Health Monitor checks the scan queue for updates, it deletes IP SLAs operations for BGP next hop neighbors that are no longer valid.</li> <li>• If the scan factor is set to 0, IP SLAs operations will not be automatically deleted by the LSP Health Monitor. This configuration is not recommended.</li> <li>• This command must be used with the <b>scan-interval</b> command.</li> </ul>
<b>Step 10</b>	<pre>force-explicit-null</pre> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-params)# force-explicit-null</p>	(Optional) Adds an explicit null label to all echo request packets of an IP SLAs operation.
<b>Step 11</b>	<pre>exp exp-bits</pre> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-params)# exp 5</p>	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 12</b>	<b>lsp-selector</b> <i>ip-address</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# lsp-selector 127.0.0.10	(Optional) Specifies the local host IP address used to select the LSP of an IP SLAs operation.
<b>Step 13</b>	<b>reply-dscp-bits</b> <i>dscp-value</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# reply-dscp-bits 5	(Optional) Specifies the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation.
<b>Step 14</b>	<b>reply-mode</b> { <b>ipv4</b>   <b>router-alert</b> }  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# reply-mode router-alert	(Optional) Specifies the reply mode for an echo request packet of an IP SLAs operation. <ul style="list-style-type: none"> <li>The default reply mode is an IPv4 UDP packet.</li> </ul>
<b>Step 15</b>	<b>request-data-size</b> <i>bytes</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# request-data-size 200	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
<b>Step 16</b>	<b>secondary-frequency</b> { <b>both</b>   <b>connection-loss</b>   <b>timeout</b> } <i>frequency</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.
<b>Step 17</b>	<b>tag</b> <i>text</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
<b>Step 18</b>	<b>threshold</b> <i>milliseconds</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# threshold 6000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
<b>Step 19</b>	<b>timeout</b> <i>milliseconds</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# timeout 7000	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
<b>Step 20</b>	<b>ttl</b> <i>time-to-live</i>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# ttl 200	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 21</b>	<b>exit</b>  <b>Example:</b> Router(config-auto-ip-sla-mpls-params)# exit	Exits MPLS parameters configuration submode and returns to global configuration mode.
<b>Step 22</b>	<b>auto ip sla mpls-lsp-monitor</b> <b>reaction-configuration</b> <i>operation-number</i> <b>react</b> { <b>connectionLoss</b>   <b>timeout</b> } [ <b>action-type</b> <i>option</i> ] [ <b>threshold-type</b> { <b>consecutive</b> [ <i>occurrences</i> ]   <b>immediate</b>   <b>never</b> }]	(Optional) Configures certain actions to occur based on events under the control of the LSP Health Monitor.
<b>Step 23</b>	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration submode and returns to privileged EXEC mode.

**Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Router****Restrictions**

- The LSP Health Monitor with LSP Discovery feature supports Layer 3 MPLS VPNs only.
- The LSP discovery option does not support IP SLAs LSP traceroute operations.
- The LSP discovery option does not support IP SLAs VCCV operations.
- The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE router. To prevent unnecessary router performance issues, careful consideration should be taken when configuring the operational and scheduling parameters of an LSP Health Monitor operation.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **mpls discovery vpn next-hop**
4. **mpls discovery vpn interval** *seconds*
5. **auto ip sla mpls-lsp-monitor** *operation-number*
6. **type echo** [*ipsla-vrf-all* | *vrf vpn-name*]
7. Configure optional parameters for the IP SLAs LSP echo operation.
8. **path-discover**
9. **hours-of-statistics-kept** *hours*
10. **force-explicit-null**
11. **interval** *milliseconds*



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

12. **lsp-selector-base** *ip-address*
13. **maximum-sessions** *number*
14. **scan-period** *minutes*
15. **session-timeout** *seconds*
16. **timeout** *seconds*
17. **exit**
18. **exit**
19. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number react lpd {lpd-group [retry number] | tree-trace} [action-type trapOnly]*
20. **ip sla logging traps**
21. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>mpls discovery vpn next-hop</b>  <b>Example:</b> Router(config)# mpls discovery vpn next-hop	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process.  <b>Note</b> This command is automatically enabled when the <b>auto ip sla mpls-lsp-monitor</b> command is entered.
<b>Step 4</b>	<b>mpls discovery vpn interval seconds</b>  <b>Example:</b> Router(config)# mpls discovery vpn interval 120	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
<b>Step 5</b>	<b>auto ip sla mpls-lsp-monitor operation-number</b>  <b>Example:</b> Router(config)# auto ip sla mpls-lsp-monitor 1	Begins configuration for an LSP Health Monitor operation and enters auto IP SLAs MPLS configuration mode.  <b>Note</b> Entering this command automatically enables the <b>mpls discovery vpn next-hop</b> command.
<b>Step 6</b>	<b>type echo [ipsla-vrf-all   vrf vpn-name]</b>  <b>Example:</b> Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all	Enters MPLS parameters configuration mode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.
<b>Step 7</b>	Configure optional parameters for the IP SLAs LSP echo operation.	(Optional) See Steps 7 through 21 in the <a href="#">“Configuring an LSP Health Monitor Operation Without LSP Discovery on a PE Router”</a> section on page 11.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 8</b>	<p><b>path-discover</b></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-params) # path-discover</p>	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters LSP discovery parameters configuration submode.
<b>Step 9</b>	<p><b>hours-of-statistics-kept</b> <i>hours</i></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # hours-of-statistics-kept 1</p>	(Optional) Sets the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.
<b>Step 10</b>	<p><b>force-explicit-null</b></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # force-explicit-null</p>	(Optional) Adds an explicit null label to all echo request packets of an LSP Health Monitor operation.
<b>Step 11</b>	<p><b>interval</b> <i>milliseconds</i></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # interval 2</p>	(Optional) Specifies the time interval between MPLS echo requests that are sent as part of the LSP discovery process for an LSP Health Monitor operation.
<b>Step 12</b>	<p><b>lsp-selector-base</b> <i>ip-address</i></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # lsp-selector-base 127.0.0.2</p>	(Optional) Specifies the base IP address used to select the LSPs belonging to the LSP discovery groups of an LSP Health Monitor operation.
<b>Step 13</b>	<p><b>maximum-sessions</b> <i>number</i></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # maximum-sessions 2</p>	<p>(Optional) Specifies the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation.</p> <p><b>Note</b> Careful consideration should be used when configuring this parameter to avoid a negative impact on the router's CPU.</p>
<b>Step 14</b>	<p><b>scan-period</b> <i>minutes</i></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # scan-period 30</p>	(Optional) Sets the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.
<b>Step 15</b>	<p><b>session-timeout</b> <i>seconds</i></p> <p><b>Example:</b> Router(config-auto-ip-sla-mpls-lpd-params) # session-timeout 60</p>	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its LSP discovery request for a particular BGP next hop neighbor.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 16</b>	<p><code>timeout seconds</code></p> <p><b>Example:</b>  Router(config-auto-ip-sla-mpls-lpd-params)#  timeout 4</p>	<p>(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its echo request packets.</p> <p><b>Note</b> Careful consideration should be used when configuring this parameter to avoid a negative impact on the router's CPU.</p>
<b>Step 17</b>	<p><code>exit</code></p> <p><b>Example:</b>  Router(config-auto-ip-sla-mpls-lpd-params)#  exit</p>	<p>Exits LSP discovery parameters configuration submode and returns to MPLS parameters configuration mode.</p>
<b>Step 18</b>	<p><code>exit</code></p> <p><b>Example:</b>  Router(config-auto-ip-sla-mpls-params)# exit</p>	<p>Exits MPLS parameters configuration mode and returns to global configuration mode.</p>
<b>Step 19</b>	<p><code>auto ip sla mpls-lsp-monitor  reaction-configuration operation-number react  lpd {lpd-group [retry number]   tree-trace}  [action-type trapOnly]</code></p> <p><b>Example:</b>  Router(config)# auto ip sla mpls-lsp-monitor  reaction-configuration 1 react lpd lpd-group  retry 3 action-type trapOnly</p>	<p>(Optional) Configures the proactive threshold monitoring parameters for an LSP Health Monitor operation with LSP discovery enabled.</p>
<b>Step 20</b>	<p><code>ip sla logging traps</code></p> <p><b>Example:</b>  Router(config)# ip sla logging traps</p>	<p>(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.</p>
<b>Step 21</b>	<p><code>exit</code></p> <p><b>Example:</b>  Router(config)# exit</p>	<p>Exits global configuration submode and returns to privileged EXEC mode.</p>

## Scheduling LSP Health Monitor Operations

### Restrictions

- All IP SLAs operations to be scheduled must be already configured.



#### Note

The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE router. Careful consideration should be taken when configuring the scheduling parameters to prevent too many IP SLAs LSP ping operations from running at the same time. The schedule period should be set to a relatively large value for large MPLS VPNs.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

Newly created IP SLAs operations (for newly discovered BGP next hop neighbors) are added to the same multioperation schedule period as the operations that are currently running. To prevent too many operations from starting at the same time, the multioperation scheduler will schedule the operations to begin at random intervals uniformly distributed over the schedule period.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh:mm:ss* | *hh:mm[:ss]* [*month day* | *day month*] | **now** | **pending**}]
4. **exit**
5. **show ip sla configuration**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>auto ip sla mpls-lsp-monitor schedule</b> <i>operation-number</i> <b>schedule-period</b> <i>seconds</i> [ <b>frequency</b> [ <i>seconds</i> ]] [ <b>start-time</b> { <b>after</b> <i>hh:mm:ss</i>   <i>hh:mm[:ss]</i> [ <i>month day</i>   <i>day month</i> ]   <b>now</b>   <b>pending</b> }]  <b>Example:</b> Router(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now	Configures the scheduling parameters for an LSP Health Monitor operation.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits to privileged EXEC mode.
<b>Step 5</b>	<b>show ip sla configuration</b>  <b>Example:</b> Router# show ip sla configuration	(Optional) Displays the IP SLAs configuration details.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****Troubleshooting Tips**

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs LSP ping or LSP traceroute operation. Use the **debug ip sla mpls-lsp-monitor** command to help troubleshoot issues with an IP SLAs LSP Health Monitor operation.

**What to Do Next**

To display the results of an individual IP SLAs operation use the **show ip sla statistics** and **show ip sla statistics aggregated** commands. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

**Manually Configuring and Scheduling an IP SLAs LSP Ping or LSP Traceroute Operation****SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **mpls lsp ping ipv4 destination-address destination-mask [force-explicit-null] [lsp-selector ip-address] [src-ip-addr source-address] [reply {dscp dscp-value | mode {ipv4 | router-alert}}]**  
or  
**mpls lsp trace ipv4 destination-address destination-mask [force-explicit-null] [lsp-selector ip-address] [src-ip-addr source-address] [reply {dscp dscp-value | mode {ipv4 | router-alert}}]**
5. **exp exp-bits**
6. **request-data-size bytes**
7. **secondary-frequency {connection-loss | timeout} frequency**
8. **tag text**
9. **threshold milliseconds**
10. **timeout milliseconds**
11. **ttl time-to-live**
12. **exit**
13. **ip sla reaction-configuration operation-number [react monitored-element] [threshold-type {never | immediate | consecutive [consecutive-occurrences] | xofy [x-value y-value] | average [number-of-probes]}] [threshold-value upper-threshold lower-threshold] [action-type {none | trapOnly | triggerOnly | trapAndTrigger}]**
14. **ip sla logging traps**
15. **ip sla schedule operation-number [life {forever | seconds}] [start-time {hh:mm[:ss] [month day | day month]}] [pending | now | after hh:mm:ss] [ageout seconds] [recurring]**
16. **exit**

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
<b>Step 3</b>	<p><b>ip sla operation-number</b></p> <p><b>Example:</b> Router(config)# ip sla 1</p>	<p>Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.</p>
<b>Step 4</b>	<p><b>mpls lsp ping ipv4 destination-address destination-mask [force-explicit-null] [lsp-selector ip-address] [src-ip-addr source-address] [reply {dscp dscp-value   mode {ipv4   router-alert}}]</b></p> <p>or</p> <p><b>mpls lsp trace ipv4 destination-address destination-mask [force-explicit-null] [lsp-selector ip-address] [src-ip-addr source-address] [reply {dscp dscp-value   mode {ipv4   router-alert}}]</b></p> <p><b>Example:</b> Router(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1</p> <p>or</p> <p><b>Example:</b> Router(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1</p>	<p>Configures the IP SLAs operation as an LSP ping operation and enters LSP ping configuration mode.</p> <p>or</p> <p>Configures the IP SLAs operation as an LSP trace operation and enters LSP trace configuration mode.</p>
<b>Step 5</b>	<p><b>exp exp-bits</b></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# exp 5</p>	<p>(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.</p> <p><b>Note</b> The LSP ping configuration mode is used in this example and in the remaining steps. Except where noted, the same commands are also supported in the LSP trace configuration mode.</p>
<b>Step 6</b>	<p><b>request-data-size bytes</b></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# request-data-size 200</p>	<p>(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.</p>

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 7</b>	<p><b>secondary-frequency</b> {<b>connection-loss</b>   <b>timeout</b>} <i>frequency</i></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# secondary-frequency connection-loss 10</p>	<p>(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.</p> <ul style="list-style-type: none"> <li>This command is for IP SLAs LSP ping operations only. LSP trace configuration mode does not support this command.</li> </ul>
<b>Step 8</b>	<p><b>tag</b> <i>text</i></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# tag testgroup</p>	<p>(Optional) Creates a user-specified identifier for an IP SLAs operation.</p>
<b>Step 9</b>	<p><b>threshold</b> <i>milliseconds</i></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# threshold 6000</p>	<p>(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.</p>
<b>Step 10</b>	<p><b>timeout</b> <i>milliseconds</i></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# timeout 7000</p>	<p>(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.</p>
<b>Step 11</b>	<p><b>ttl</b> <i>time-to-live</i></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# ttl 200</p>	<p>(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.</p>
<b>Step 12</b>	<p><b>exit</b></p> <p><b>Example:</b> Router(config-sla-monitor-lspPing)# exit</p>	<p>Exits LSP ping or LSP trace configuration submode and returns to global configuration mode.</p>
<b>Step 13</b>	<p><b>ip sla reaction-configuration</b> <i>operation-number</i> [<b>react</b> <i>monitored-element</i>] [<b>threshold-type</b> {<b>never</b>   <b>immediate</b>   <b>consecutive</b> [<i>consecutive-occurrences</i>]   <b>xofy</b> [<i>x-value</i> <i>y-value</i>]   <b>average</b> [<i>number-of-probes</i>]}] [<b>threshold-value</b> <i>upper-threshold</i> <i>lower-threshold</i>] [<b>action-type</b> {<b>none</b>   <b>trapOnly</b>   <b>triggerOnly</b>   <b>trapAndTrigger</b>}]</p> <p><b>Example:</b> Router(config)# ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type traponly</p>	<p>(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.</p>
<b>Step 14</b>	<p><b>ip sla logging traps</b></p> <p><b>Example:</b> Router(config)# ip sla logging traps</p>	<p>(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.</p>



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 15</b>	<pre><b>ip sla schedule</b> <i>operation-number</i> [<b>life</b> {<b>forever</b>   <i>seconds</i>}] [<b>start-time</b> {<i>hh:mm[:ss]</i> [<i>month day</i>   <i>day month</i>]   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i>}] [<b>ageout</b> <i>seconds</i>] [<b>recurring</b>]</pre> <p><b>Example:</b> Router(config)# ip sla schedule 1 start-time now</p>	Configures the scheduling parameters for an IP SLAs operation.
<b>Step 16</b>	<pre><b>exit</b></pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration submode and returns to privileged EXEC mode.

## Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs LSP ping or LSP traceroute operation.

## What to Do Next

To display the results of an individual IP SLAs operation use the **show ip sla statistics** and **show ip sla statistics aggregated** commands. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

## Manually Configuring and Scheduling an IP SLAs VCCV Operation

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **mpls lsp ping pseudowire** *peer-ipaddr vc-id* [**source-ipaddr** *source-ipaddr*]
5. **exp** *exp-bits*
6. **frequency** *seconds*
7. **request-data-size** *bytes*
8. **secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency*
9. **tag** *text*
10. **threshold** *milliseconds*
11. **timeout** *milliseconds*
12. **exit**

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

13. **ip sla reaction-configuration** *operation-number* [**react** *monitored-element*] [**threshold-type** {**never** | **immediate** | **consecutive** [*consecutive-occurrences*] | **xofy** [*x-value y-value*] | **average** [*number-of-probes*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**}]
14. **ip sla logging traps**
15. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*month day | day month*] | **pending** | **now** | **after** *hh:mm:ss*}] [**ageout** *seconds*] [**recurring**]
16. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip sla</b> <i>operation-number</i>  <b>Example:</b> Router(config)# ip sla 777	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
<b>Step 4</b>	<b>mpls lsp ping pseudowire</b> <i>peer-ipaddr vc-id</i> [ <b>source-ipaddr</b> <i>source-ipaddr</i> ]  <b>Example:</b> Router(config-ip-sla)# mpls lsp ping pseudowire 192.168.1.103 123 source-ipaddr 192.168.1.102	Configures the IP SLAs operation as an LSP pseudo-wire ping and enters VCCV configuration mode.
<b>Step 5</b>	<b>exp</b> <i>exp-bits</i>  Router(config-sla-vccv)# exp 5	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation.
<b>Step 6</b>	<b>frequency</b> <i>seconds</i>  <b>Example:</b> Router(config-sla-vccv)# frequency 120	(Optional) Specifies the rate at which a specified IP SLAs operation repeats.
<b>Step 7</b>	<b>request-data-size</b> <i>bytes</i>  <b>Example:</b> Router(config-sla-vccv)# request-data-size 200	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation.
<b>Step 8</b>	<b>secondary-frequency</b> { <b>both</b>   <b>connection-loss</b>   <b>timeout</b> } <i>frequency</i>  <b>Example:</b> Router(config-sla-vccv)# secondary-frequency connection-loss 10	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 9</b>	<p><b>tag</b> <i>text</i></p> <p><b>Example:</b> Router(config-sla-vccv)# tag testgroup</p>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
<b>Step 10</b>	<p><b>threshold</b> <i>milliseconds</i></p> <p>Router(config-sla-vccv)# threshold 6000</p>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
<b>Step 11</b>	<p><b>timeout</b> <i>milliseconds</i></p> <p><b>Example:</b> Router(config-sla-vccv)# timeout 7000</p>	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet.
<b>Step 12</b>	<p><b>exit</b></p> <p><b>Example:</b> Router(config-sla-vccv)# exit</p>	Exits VCCV configuration mode and returns to global configuration mode.
<b>Step 13</b>	<p><b>ip sla reaction-configuration</b> <i>operation-number</i> [<b>react</b> <i>monitored-element</i>] [<b>threshold-type</b> {<b>never</b>   <b>immediate</b>   <b>consecutive</b> [<i>consecutive-occurrences</i>]   <b>xofy</b> [<i>x-value</i> <i>y-value</i>]   <b>average</b> [<i>number-of-probes</i>]}] [<b>threshold-value</b> <i>upper-threshold</i> <i>lower-threshold</i>] [<b>action-type</b> {<b>none</b>   <b>trapOnly</b>   <b>triggerOnly</b>   <b>trapAndTrigger</b>}]</p> <p><b>Example:</b> Router(config)# ip sla reaction-configuration 777 react connectionLoss threshold-type consecutive 3 action-type traponly</p>	(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.
<b>Step 14</b>	<p><b>ip sla logging traps</b></p> <p><b>Example:</b> Router(config)# ip sla logging traps</p>	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
<b>Step 15</b>	<p><b>ip sla schedule</b> <i>operation-number</i> [<b>life</b> {<b>forever</b>   <i>seconds</i>}] [<b>start-time</b> {<i>hh:mm[:ss]</i> [<i>month</i> <i>day</i>   <i>day</i> <i>month</i>]   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i>}] [<b>ageout</b> <i>seconds</i>] [<b>recurring</b>]</p> <p><b>Example:</b> Router(config)# ip sla schedule 777 life forever start-time now</p>	Configures the scheduling parameters for an IP SLAs operation.
<b>Step 16</b>	<p><b>exit</b></p> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration submode and returns to privileged EXEC mode.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****Troubleshooting Tips**

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an individual IP SLAs PWE3 service via VCCV operation.

**What to Do Next**

To display the results of an individual IP SLAs operation use the **show ip sla statistics** and **show ip sla statistics aggregated** commands. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

**Verifying and Troubleshooting LSP Health Monitor Operations****SUMMARY STEPS**

1. **debug ip sla error** *[operation-number]*
2. **debug ip sla mpls-lsp-monitor** *[operation-number]*
3. **debug ip sla trace** *[operation-number]*
4. **show ip sla mpls-lsp-monitor collection-statistics** *[group-id]*
5. **show ip sla mpls-lsp-monitor configuration** *[operation-number]*
6. **show ip sla mpls-lsp-monitor lpd operational-state** *[group-id]*
7. **show ip sla mpls-lsp-monitor neighbors**
8. **show ip sla mpls-lsp-monitor scan-queue** *operation-number*
9. **show ip sla mpls-lsp-monitor summary** *[operation-number [group [group-id]]]*
10. **show ip sla statistics** *[operation-number] [details]*
11. **show ip sla statistics aggregated** *[operation-number] [details]*
12. **show mpls discovery vpn**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>debug ip sla error</b> <i>[operation-number]</i>  <b>Example:</b> Router# debug ip sla error	(Optional) Enables debugging output of IP SLAs operation run-time errors.
<b>Step 2</b>	<b>debug ip sla mpls-lsp-monitor</b> <i>[operation-number]</i>  <b>Example:</b> Router# debug ip sla mpls-lsp-monitor	(Optional) Enables debugging output of LSP Health Monitor operations.
<b>Step 3</b>	<b>debug ip sla trace</b> <i>[operation-number]</i>  <b>Example:</b> Router# debug ip sla trace	(Optional) Enables debugging output for tracing the execution of IP SLAs operations.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 4</b>	<pre>show ip sla mpls-lsp-monitor collection-statistics [group-id]</pre> <p><b>Example:</b> Router# show ip sla mpls-lsp-monitor collection-statistics 100001</p>	<p>(Optional) Displays the statistics for IP SLAs operations belonging to an LSP discovery group of an LSP Health Monitor operation.</p> <p><b>Note</b> This command is applicable only if the LSP discovery option is enabled.</p>
<b>Step 5</b>	<pre>show ip sla mpls-lsp-monitor configuration [operation-number]</pre> <p><b>Example:</b> Router# show ip sla mpls-lsp-monitor configuration 1</p>	<p>(Optional) Displays configuration settings for LSP Health Monitor operations.</p>
<b>Step 6</b>	<pre>show ip sla mpls-lsp-monitor lpd operational-state [group-id]</pre> <p><b>Example:</b> Router# show ip sla mpls-lsp-monitor lpd operational-state 100001</p>	<p>(Optional) Displays the operational status of the LSP discovery groups belonging to an LSP Health Monitor operation.</p> <p><b>Note</b> This command is applicable only if the LSP discovery option is enabled.</p>
<b>Step 7</b>	<pre>show ip sla mpls-lsp-monitor neighbors</pre> <p><b>Example:</b> Router# show ip sla mpls-lsp-monitor neighbors</p>	<p>(Optional) Displays routing and connectivity information about MPLS VPN BGP next hop neighbors discovered by the LSP Health Monitor operation.</p>
<b>Step 8</b>	<pre>show ip sla mpls-lsp-monitor scan-queue operation-number</pre> <p><b>Example:</b> Router# show ip sla mpls-lsp-monitor scan-queue 1</p>	<p>(Optional) Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an LSP Health Monitor operation.</p>
<b>Step 9</b>	<pre>show ip sla mpls-lsp-monitor summary [operation-number [group [group-id]]]</pre> <p><b>Example:</b> Router# show ip sla mpls-lsp-monitor summary</p>	<p>(Optional) Displays BGP next hop neighbor and LSP discovery group information for LSP Health Monitor operations.</p> <p><b>Note</b> This command is applicable only if the LSP discovery option is enabled.</p>
<b>Step 10</b>	<pre>show ip sla statistics [operation-number] [details]</pre> <p><b>Example:</b> Router# show ip sla statistics 100001</p>	<p>(Optional) Displays the current operational status and statistics of all IP SLAs operations or a specified operation.</p> <p><b>Note</b> This command applies only to manually configured IP SLAs operations.</p>

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

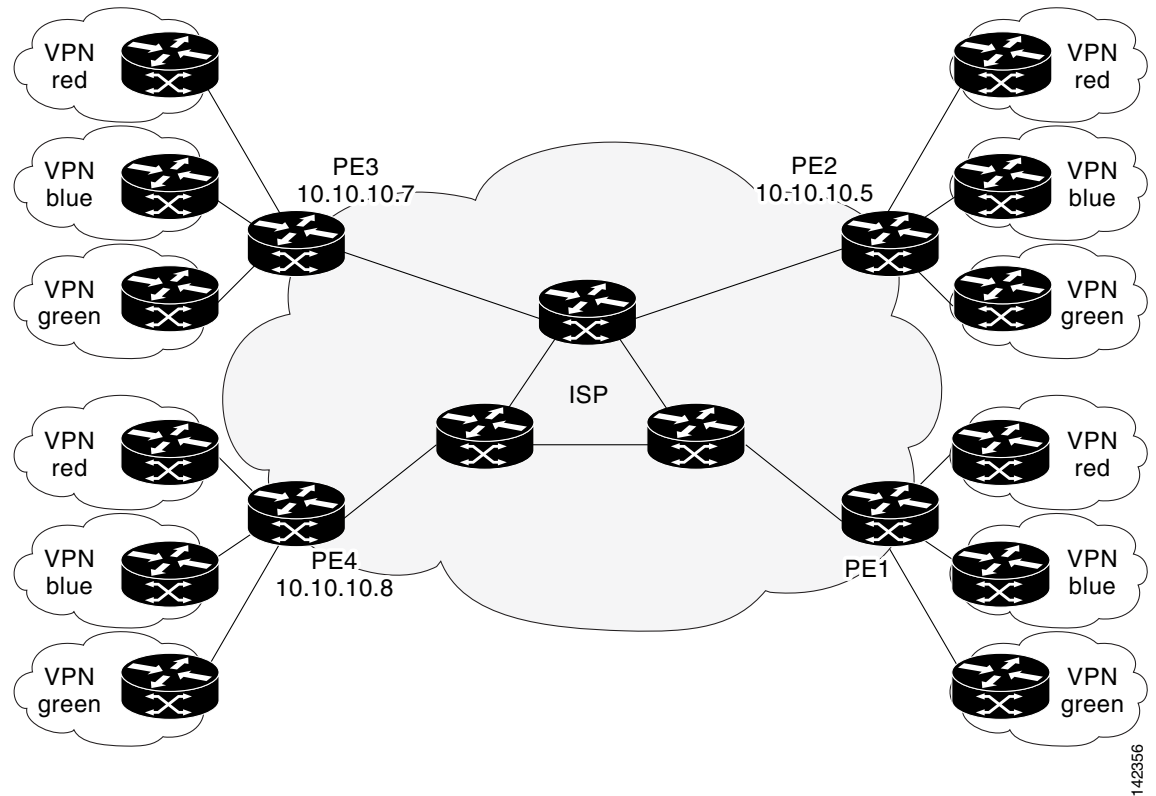
	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 11</b>	<b>show ip sla statistics aggregated</b> [operation-number] [details]	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.
	<b>Example:</b> Router# show ip sla statistics aggregated 100001	<b>Note</b> This command applies only to manually configured IP SLAs operations.
<b>Step 12</b>	<b>show mpls discovery vpn</b>	(Optional) Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.
	<b>Example:</b> Router# show mpls discovery vpn	

## Configuration Examples for the LSP Health Monitor

- [Example: Configuring and Verifying the LSP Health Monitor Without LSP Discovery, page 28](#)
- [Example: Configuring and Verifying the LSP Health Monitor with LSP Discovery, page 32](#)
- [Example: Manually Configuring an IP SLAs LSP Ping Operation, page 35](#)
- [Example: Manually Configuring an IP SLAs VCCV Operation, page 36](#)

### Example: Configuring and Verifying the LSP Health Monitor Without LSP Discovery

Figure 4 illustrates a simple VPN scenario for an ISP. This network consists of a core MPLS VPN with four PE routers belonging to three VPNs: red, blue, and green. From the perspective of router PE1, these VPNs are reachable remotely through BGP next hop routers PE2 (router ID: 10.10.10.5), PE3 (router ID: 10.10.10.7), and PE4 (router ID: 10.10.10.8).

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****Figure 4 Network Used for LSP Health Monitor Example**

142356

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on router PE1 (see Figure 4) using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors (PE2, PE3, and PE4) in use by all VRFs (red, blue, and green) associated with router PE1. The BGP next hop neighbor process is enabled, and the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database is set to 60 seconds. The time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute. The secondary frequency option is enabled for both connection loss and timeout events, and the secondary frequency is set to 10 seconds. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss or timeout events occur, an SNMP trap notification is sent. Multioperation scheduling and the generation of IP SLAs SNMP system logging messages are enabled.

**Router PE1 Configuration**

```

mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
  type echo ipsla-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency both 10
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly

```



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

```

auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type
consecutive 3 action-type trapOnly

ip sla traps
snmp-server enable traps rtr
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

The following is sample output from the **show ip sla mpls-lsp-monitor configuration** command for router PE1:

```

PE1# show ip sla mpls-lsp-monitor configuration 1

Entry Number : 1
Modification time : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type : echo
Vrf Name : ipsla-vrf-all
Tag :
EXP Value : 0
Timeout(ms) : 1000
Threshold(ms) : 5000
Frequency(sec) : Equals schedule period
LSP Selector : 127.0.0.1
ScanInterval(min) : 1
Delete Scan Factor : 1
Operations List : 100001-100003
Schedule Period(sec): 60
Request size : 100
Start Time : Start Time already passed
SNMP RowStatus : Active
TTL value : 255
Reply Mode : ipv4
Reply Dscp Bits :
Secondary Frequency : Enabled on Timeout
Value(sec) : 10
Reaction Configs :
  Reaction : connectionLoss
  Threshold Type : Consecutive
  Threshold Count : 3
  Action Type : Trap Only
  Reaction : timeout
  Threshold Type : Consecutive
  Threshold Count : 3
  Action Type : Trap Only

```

The following is sample output from the **show mpls discovery vpn** command for router PE1:

```

PE1# show mpls discovery vpn

Refresh interval set to 60 seconds.
Next refresh in 46 seconds

Next hop 10.10.10.5 (Prefix: 10.10.10.5/32)
  in use by: red, blue, green

Next hop 10.10.10.7 (Prefix: 10.10.10.7/32)
  in use by: red, blue, green

Next hop 10.10.10.8 (Prefix: 10.10.10.8/32)
  in use by: red, blue, green

```

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

The following is sample output from the **show ip sla mpls-lsp-monitor neighbors** command for router PE1:

```
PE1# show ip sla mpls-lsp-monitor neighbors

IP SLA MPLS LSP Monitor Database : 1
BGP Next hop 10.10.10.5 (Prefix: 10.10.10.5/32) OK
  ProbeID: 100001 (red, blue, green)
BGP Next hop 10.10.10.7 (Prefix: 10.10.10.7/32) OK
  ProbeID: 100002 (red, blue, green)
BGP Next hop 10.10.10.8 (Prefix: 10.10.10.8/32) OK
  ProbeID: 100003 (red, blue, green)
```

The following is sample output from the **show ip sla mpls-lsp-monitor scan-queue 1** and **debug ip sla mpls-lsp-monitor** commands when IP connectivity from router PE1 to router PE4 is lost. This output shows that connection loss to each of the VPNs associated with router PE4 (red, blue, and green) was detected and that this information was added to the LSP Health Monitor scan queue. Also, since router PE4 is no longer a valid BGP next hop neighbor, the IP SLAs operation for router PE4 (Probe 10003) is being deleted.

```
PE1# show ip sla mpls-lsp-monitor scan-queue 1

Next scan Time after: 20 Secs
Next Delete scan Time after: 20 Secs

BGP Next hop      Prefix          vrf              Add/Delete?
10.10.10.8        0.0.0.0/0      red              Del(100003)
10.10.10.8        0.0.0.0/0      blue             Del(100003)
10.10.10.8        0.0.0.0/0      green            Del(100003)
```

```
PE1# debug ip sla mpls-lsp-monitor

IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:48: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf red from tree entry 10.10.10.8
*Aug 19 19:56: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:56: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in DeleteQ(1)
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf blue from tree entry 10.10.10.8
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing vrf green from tree entry 10.10.10.8
*Aug 19 19:49: IP SLAs MPLSLM(1):Removing Probe 100003
```

The following is sample output from the **show ip sla mpls-lsp-monitor scan-queue 1** and **debug ip sla mpls-lsp-monitor** commands when IP connectivity from router PE1 to router PE4 is restored. This output shows that each of the VPNs associated with router PE4 (red, blue, and green) were discovered and that this information was added to the LSP Health Monitor scan queue. Also, since router PE4 is a newly discovered BGP next hop neighbor, a new IP SLAs operation for router PE4 (Probe 100005) is being created and added to the LSP Health Monitor multioperation schedule. Even though router PE4 belongs to three VPNs, only one IP SLAs operation is being created.

```
PE1# show ip sla mpls-lsp-monitor scan-queue 1

Next scan Time after: 23 Secs
Next Delete scan Time after: 23 Secs

BGP Next hop      Prefix          vrf              Add/Delete?
10.10.10.8        10.10.10.8/32  red              Add
10.10.10.8        10.10.10.8/32  blue             Add
10.10.10.8        10.10.10.8/32  green            Add
```

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

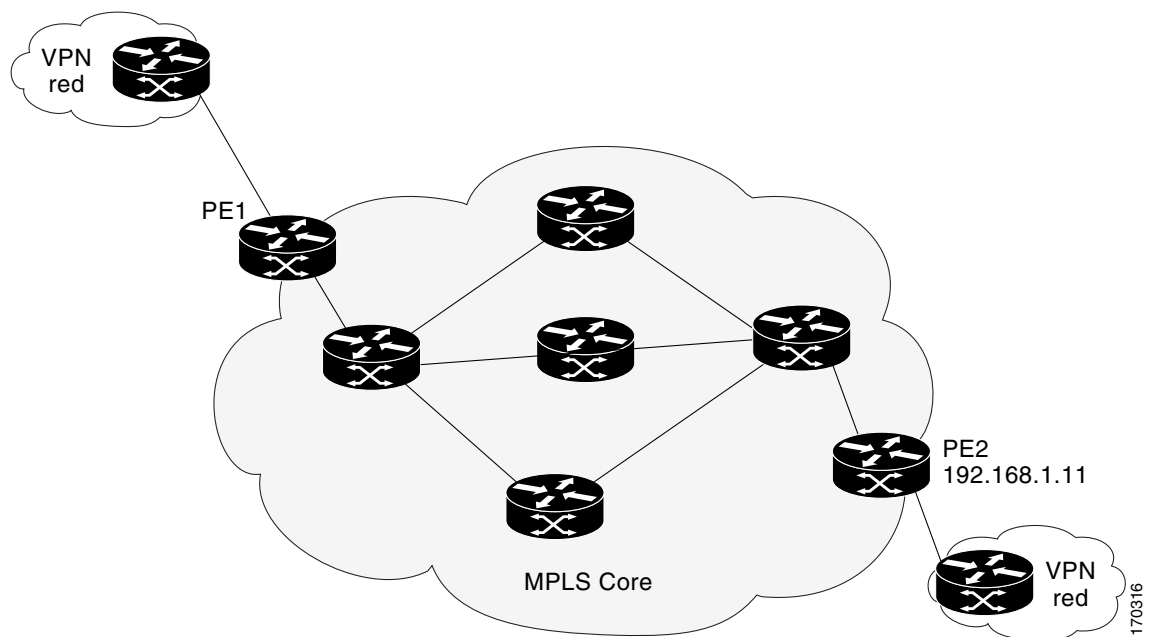
```
PE1# debug ip sla mpls-lsp-monitor
```

```
IP SLAs MPLSLM debugging for all entries is on
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Next hop 10.10.10.8 added in AddQ
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf red into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding Probe 100005
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding ProbeID 100005 to tree entry 10.10.10.8 (1)
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf blue into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Adding vrf green into tree entry 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Duplicate in AddQ 10.10.10.8
*Aug 19 19:59: IP SLAs MPLSLM(1):Added Probe(s) 100005 will be scheduled after 26 secs
over schedule period 60
```

**Example: Configuring and Verifying the LSP Health Monitor with LSP Discovery**

Figure 5 illustrates a simple VPN scenario for an ISP. This network consists of a core MPLS VPN with two PE routers belonging to a VPN named red. From the perspective of router PE1, there are three equal-cost multipaths available to reach router PE2.

**Figure 5** Network Used for LSP Health Monitor with LSP Discovery Example



The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on router PE1 (see Figure 5) using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 100. Operation 100 is configured to automatically create IP SLAs LSP ping operations for all equal-cost multipaths between router PE1 and router PE2. The BGP next hop neighbor process is enabled, and the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database is set to 30 seconds. The time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute. The secondary frequency option is enabled for both connection loss

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

and timeout events, and the secondary frequency is set to 5 seconds. The explicit null label option for echo request packets is enabled. The LSP rediscovery time period is set to 3 minutes. As specified by the proactive threshold monitoring configuration, an SNMP trap notification will be sent when an LSP discovery group status changes occurs. Multioperation scheduling and the generation of IP SLAs SNMP system logging messages are enabled.

**Router PE1 Configuration**

```

mpls discovery vpn next-hop
mpls discovery vpn interval 30
!
auto ip sla mpls-lsp-monitor 100
  type echo ipsla-vrf-all
  scan-interval 1
  secondary-frequency both 5
!
  path-discover
  force-explicit-null
  scan-period 3
!
auto ip sla mpls-lsp-monitor reaction-configuration 100 react lpd-group retry 3
action-type trapOnly
!
auto ip sla mpls-lsp-monitor schedule 100 schedule-period 30 start-time now
!
ip sla logging traps
snmp-server enable traps rtr

```

The following is sample output from the **show ip sla mpls-lsp-monitor configuration** command for router PE1:

```

PE1# show ip sla mpls-lsp-monitor configuration

Entry Number : 100
Modification time   : *21:50:16.411 GMT Tue Jun 20 2006
Operation Type     : echo
Vrf Name          : ipsla-vrf-all
Tag               :
EXP Value         : 0
Timeout(ms)       : 5000
Threshold(ms)     : 50
Frequency(sec)    : Equals schedule period
ScanInterval(min) : 1
Delete Scan Factor : 1
Operations List    : 100002
Schedule Period(sec) : 30
Request size      : 100
Start Time        : Start Time already passed
SNMP RowStatus    : Active
TTL value         : 255
Reply Mode        : ipv4
Reply Dscp Bits   :
Path Discover     : Enable
  Maximum sessions : 1
  Session Timeout(seconds) : 120
  Base LSP Selector : 127.0.0.0
  Echo Timeout(seconds) : 5
  Send Interval(msec) : 0
  Label Shimming Mode : force-explicit-null
  Number of Stats Hours : 2
  Scan Period(minutes) : 3
Secondary Frequency : Enabled on Connection Loss and Timeout

```

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

```

Value(sec) : 5
Reaction Configs :
  Reaction : Lpd Group
  Retry Number : 3
  Action Type : Trap Only

```

The following is sample output from the **show mpls discovery vpn** command for router PE1:

```

PE1# show mpls discovery vpn

Refresh interval set to 30 seconds.
Next refresh in 4 seconds

Next hop 192.168.1.11 (Prefix: 192.168.1.11/32)
      in use by: red

```

The following is sample output from the **show ip sla mpls-lsp-monitor neighbors** command for router PE1:

```

PE1# show ip sla mpls-lsp-monitor neighbors

IP SLA MPLS LSP Monitor Database : 100
BGP Next hop 192.168.1.11 (Prefix: 192.168.1.11/32) OK Paths: 3
  ProbeID: 100001 (red)

```

The following is sample output from the **show ip sla mpls-lsp-monitor lpd operational-state** command for LSP discovery group 100001:

```

PE1# show ip sla mpls-lsp-monitor lpd operational-state

Entry number: 100001
MPLSLM Entry Number: 100
Target FEC Type: LDP IPv4 prefix
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :

```

Path Index	Outgoing Interface	Lsp Selector	Link Type	Conn Id	Adj Addr	Downstream Label Stack	Status
1	Et0/0	127.0.0.8	90	0	10.10.18.30	21	OK
2	Et0/0	127.0.0.2	90	0	10.10.18.30	21	OK
3	Et0/0	127.0.0.1	90	0	10.10.18.30	21	OK

The following is sample output from the **show ip sla mpls-lsp-monitor collection-statistics** command for LSP discovery group 100001:

```

PE1# show ip sla mpls-lsp-monitor collection-statistics

Entry number: 100001
Start Time Index: *21:52:59.795 GMT Tue Jun 20 2006
Path Discovery Start Time: *22:08:04.507 GMT Tue Jun 20 2006
Target Destination IP address: 192.168.1.11
Path Discovery Status: OK
Path Discovery Completion Time: 3052

```

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

```

Path Discovery Minimum Paths: 3
Path Discovery Maximum Paths: 3
LSP Group Index: 100002
LSP Group Status: up
Total Pass: 36
Total Timeout: 0          Total Fail: 0
Latest Probe Status: 'up,up,up'
Latest Path Identifier: '127.0.0.8-Et0/0-21,127.0.0.2-Et0/0-21,127.0.0.1-Et0/0-21'
Minimum RTT: 280          Maximum RTT: 324          Average RTT: 290

```

The following is sample output from the **show ip sla mpls-lsp-monitor summary** command for LSP Health Monitor operation 100:

```

PE1# show ip sla mpls-lsp-monitor summary 100

Index          - MPLS LSP Monitor probe index
Destination    - Target IP address of the BGP next hop
Status         - LPD group status
LPD Group ID   - Unique index to identify the LPD group
Last Operation Time - Last time an operation was attempted by
                  a particular probe in the LPD Group

Index  Destination    Status    LPD Group ID    Last Operation Time
100    192.168.1.11    up        100001          *22:20:29.471 GMT Tue Jun 20 2006

```

The following is sample output from the **show ip sla mpls-lsp-monitor summary** command for LSP discovery group 100001:

```

PE1#show ip sla mpls-lsp-monitor summary 100 group 100001

Group ID          - unique number to identify a LPD group
Lsp-selector      - Unique 127/8 address used to identify a LPD
Last Operation status - Latest probe status
Last RTT         - Latest Round Trip Time
Last Operation Time - Time when the last operation was attempted

Group ID  Lsp-Selector    Status    Failures    Successes    RTT    Last Operation Time
100001    127.0.0.8       up        0           55           320    *22:20:29.471 GMT Tue
Jun 20 2006
100001    127.0.0.2       up        0           55           376    *22:20:29.851 GMT Tue
Jun 20 2006
100001    127.0.0.1       up        0           55           300    *22:20:30.531 GMT Tue
Jun 20 2006

```

**Example: Manually Configuring an IP SLAs LSP Ping Operation**

The following example shows how to manually configure and schedule an IP SLAs LSP ping operation:

```

ip sla 1
mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1
frequency 120
secondary-frequency timeout 30
!
ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3
action-type trapOnly
ip sla reaction-configuration 1 react timeout threshold-type consecutive 3 action-type
trapOnly
ip sla logging traps
!
ip sla schedule 1 start-time now life forever

```

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****Example: Manually Configuring an IP SLAs VCCV Operation**

The following example shows how to manually configure an IP SLAs VCCV operation in conjunction with the proactive threshold monitoring and multioperation scheduling capabilities of the LSP Health Monitor.

In this example, a VC with the identifier 123 has already been established between the PE router and its peer at IP address 192.168.1.103.

IP SLAs VCCV operation 777 is configured with operation parameters and reaction conditions, and it is scheduled to begin immediately and run indefinitely.

```
ip sla 777
mpls lsp ping pseudowire 192.168.1.103 123
  exp 5
  frequency 120
  secondary-frequency timeout 30
  tag testgroup
  threshold 6000
  timeout 7000
  exit
!
ip sla reaction-configuration 777 react rtt threshold-value 6000 3000 threshold-type
immediate 3 action-type traponly
ip sla reaction-configuration 777 react connectionLoss threshold-type immediate
action-type traponly
ip sla reaction-configuration 777 react timeout threshold-type consecutive 3 action-type
traponly
ip sla logging traps
!
ip sla schedule 777 life forever start-time now
exit
```

**RTT Thresholds**

The **threshold** command configures 6000 milliseconds as the amount of time for a rising threshold to be declared on the monitored pseudo-wire. The first **ip sla reaction-configuration** command specifies that an SNMP logging trap is to be sent immediately if the round-trip time violates the upper threshold of 6000 milliseconds or the lower threshold of 3000 milliseconds.

**Connection Loss**

The second **ip sla reaction-configuration** command specifies that an SNMP logging trap is to be sent immediately if a connection loss occurs for the monitored pseudo-wire.

**Response Timeout**

The **timeout** command configures 7000 seconds as the amount of time that VCCV operation 777 waits for a response from its request packet before a timeout is declared. The **secondary-frequency** command specifies that, if a timeout occurs, the measurement frequency of the operation repeats is to be increased from 120 seconds (the initial measurement frequency specified using the **frequency** command) to a faster rate of 30 seconds. The third **ip sla reaction-configuration** command specifies that an SNMP logging trap is to be sent if three consecutive timeouts occur.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

# Additional References

## Related Documents

Related Topic	Document Title
MPLS LSP ping and LSP traceroute management tools	<a href="#">MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV</a> , Cisco IOS feature
MPLS LSP discovery management tool	<a href="#">MPLS EM—MPLS LSP Multipath Tree Trace</a> , Cisco IOS feature
Configuring standard IP access lists	“ <a href="#">Creating an IP Access List and Applying It to an Interface</a> ” chapter of the <i>Cisco IOS Security Configuration Guide</i>
Multioperation scheduling for Cisco IOS IP SLAs	“ <a href="#">Configuring Multioperation Scheduling of IP SLAs Operations</a> ” chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i>
Proactive threshold monitoring for Cisco IOS IP SLAs	“ <a href="#">Configuring Proactive Threshold Monitoring of IP SLAs Operations</a> ” chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i>
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS IP SLAs commands	<a href="#">Cisco IOS IP SLAs Command Reference</a>

## Standards

Standard	Title
draft-ietf-mpls-lsp-ping-09.txt	Detecting MPLS Data Plane Failures
draft-ietf-mpls-oam-frmwk-03.txt	A Framework for MPLS Operations and Management (OAM)
draft-ietf-mpls-oam-requirements-06.txt	OAM Requirements for MPLS Networks

## MIBs

MIB	MIBs Link
CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****RFCs**

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

**Technical Assistance**

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

# Feature Information for LSP Health Monitor Operations

Table 2 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 2 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 2** Feature Information for the LSP Health Monitor

Feature Name	Releases	Feature Information
IP SLAs—LSP Health Monitor	12.2(27)SBC 12.2(28)SB 12.2(33)SRA 12.4(6)T 15.0(1)S Cisco IOS XE 3.1.0SG	The IP SLAs LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs.
IP SLAs—LSP Health Monitor	12.2(31)SB2 12.2(33)SB 12.2(33)SRB	For software releases in which this feature was already introduced, new command-line interface (CLI) was implemented that replaces the CLI introduced in the earlier releases.
IP SLAs—LSP Health Monitor with LSP Discovery	12.2(31)SB2 12.2(33)SRB 15.0(1)S Cisco IOS XE 3.1.0SG 12.2(50)SY	<p>The LSP discovery capability was added.</p> <p>In Cisco IOS Release 12.2(50)SY, support of IP SLAs LSP Health Monitor with LSP Discovery was added.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">The LSP Discovery Process, page 5</a></li> <li>• <a href="#">Configuring the LSP Health Monitor Operation with LSP Discovery on a PE Router, page 15</a></li> </ul> <p>The following commands were introduced or modified: <b>show ip sla mpls lpd operation statistics, show ip sla mpls summary.</b></p>
IP SLAs for MPLS Pseudo Wire (PWE3) via VCCV	12.2(33)SB 12.2(33)SRC 15.0(1)S Cisco IOS XE 3.1.0SG	The IP SLAs VCCV operation was added to support Virtual Circuit Connectivity Verification (VCCV) for Pseudo-Wire Emulation Edge-to-Edge (PWE3) services across MPLS networks.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

***EFT REVIEW DRAFT – CISCO CONFIDENTIAL***

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007-2010 Cisco Systems, Inc. All rights reserved.