IP SLAs—LSP Health Monitor

First Published: August 21, 2007
Last Updated: June 2, 2010

The IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor feature provides the capability to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (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 or LSP traceroute operations based on network topology.

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

Finding Feature Information in This Module

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 the LSP Health Monitor" section on page 22.

Use Cisco Feature Navigator to find information about platform support and Cisco 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

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

© <year> Cisco Systems, Inc. All rights reserved.

Prerequisites for the LSP Health Monitor

The participating PE routers 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.

For more information about the MPLS LSP Ping feature, see the "Related Documents" section on page 20.

Note The destination PE routers do not require the IP SLAs Responder to be enabled.

Restrictions for the LSP Health Monitor

The Cisco IOS Release 12.2(27)SBC, Release 12.2(33)SRA, and Release 12.2(33)SXH implementation of the LSP Health Monitor feature supports only Layer 3 MPLS VPNs. These software releasse also support only single path connectivity measurements between the source PE router and associated Border Gateway Protocol (BGP) next hop neighbors.

Information About the LSP Health Monitor

Benefits of the LSP Health Monitor

The LSP Health Monitor feature provides the following key benefits:

- End-to-end LSP connectivity measurements for determining network availability or testing network connectivity in MPLS networks
- Proactive threshold violation monitoring through SNMP trap notifications and syslog messages
- Reduced network troubleshooting time for MPLS networks
- Scalable network error detection using fast retry capability
- Creation and deletion of IP SLAs LSP ping and LSP traceroute operations based on network topology
- Discovery of BGP next hop neighbors based on local VPN routing or forwarding instances (VRFs) and global routing tables

- Multioperation scheduling of IP SLAs operations

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 enables the BGP next hop neighbor discovery process on a given PE router.

   When this process is enable, 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.

2. The user configures an LSP Health Monitor operation.

   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.

3. The user configures proactive threshold violation monitoring for the LSP Health Monitor operation.
4. The user configures multioperation scheduling parameters for the LSP Health Monitor operation.
5. Depending on the configuration options chosen, the LSP Health Monitor automatically creates individual IP SLAs LSP ping or LSP traceroute operations for each applicable BGP next hop neighbor.

   For any given LSP Health Monitor operation, only one IP SLAs LSP ping or LSP traceroute operation will be configured per BGP next hop neighbor. However, more than one LSP Health Monitor operation can be running on a particular PE router at the same time (for more details, see the note at the end of this section).

6. Each IP SLAs LSP ping or LSP traceroute operation measures network connectivity between the source PE router and the discovered destination PE router.

Note More than one LSP Health Monitor operation can be running on a particular PE router at the same time. For example, one LSP Health Monitor operation can be configured to discover BGP next hop neighbors belonging to the VRF named VPN1. On the same PE router, another LSP Health Monitor operation can be configured to discover neighbors belonging to the VRF named VPN2. In this case, if a BGP next hop neighbor belonged to both VPN1 and VPN2, then the PE router would create two IP SLAs operations for this neighbor—one for VPN1 and one for VPN2.

Adding and Deleting IP SLAs Operations from the LSP Health Monitor Database

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.

Access Lists for Filtering BGP Next Hop Neighbors

Standard IP access lists can be configured (using the **access-list** [IP standard] command in global configuration mode) 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.

For more information about configuring standard IP access lists, see the "Related Documents" section on page 20.

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.

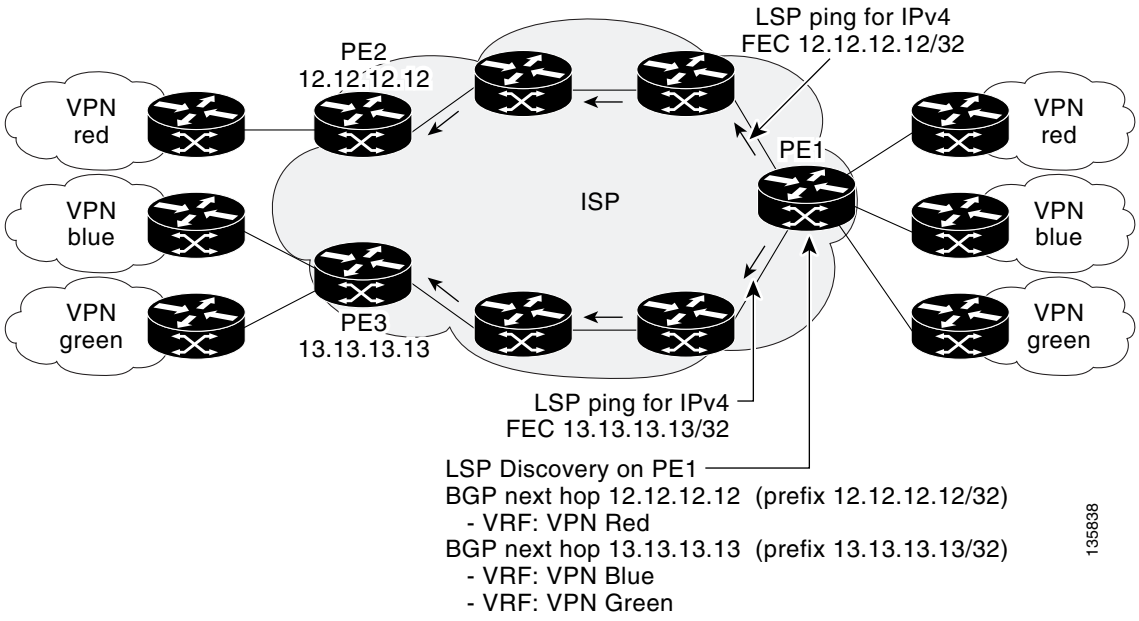
Discovery of Neighboring PE Routers

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 immediately to the database. However, BGP next hop neighbors (that are no longer valid) are only removed from the database periodically as defined by the user.

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 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. For more information about the MPLS LSP Ping feature, see the "Related Documents" section on page 20.

Figure 1 BGP Next Hop Neighbor Discovery for a Simple VPN



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.

For more information on how to configure IP SLAs LSP ping or LSP traceroute operations using the LSP Health Monitor, see the "Configuring the LSP Health Monitor on a Source PE Router" section on page 6. For more information on how to manually configure an individual IP SLAs LSP ping or LSP traceroute operation, see the "Manually Configuring an IP SLAs LSP Ping or LSP Traceroute Operation" section on page 11.

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. For more information about the MPLS LSP Ping and MPLS LSP Traceroute features, see the "Related Documents" section on page 20.

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. For more information about proactive threshold monitoring for Cisco IOS IP SLAs, see the "Related Documents" section on page 20.

With the introduction of the LSP Health Monitor feature, a new operation 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 LSP, the frequency at which the failed LSP 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.

Note 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. For more information about scheduling a group of standard IP SLAs operations, see the "Related Documents" section on page 20.

How to Use the LSP Health Monitor

Configuring the LSP Health Monitor on a Source PE Router

Perform this task to configure the operation parameters, reaction conditions, and scheduling options for an LSP Health Monitor operation. The IP SLAs measurement statistics are stored on the source PE router.

Prerequisites

The LSP Health Monitor must be configured on a PE router.

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** [**saa-vrf-all** | **vrf** *vpn-name*]
   or
   type pathEcho [**saa-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*
13. **reply-dscp-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. **ttl** *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. **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**}]
24. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls discovery vpn next-hop** **Example:** `Router(config)# mpls discovery vpn next-hop`	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process. **Note** This command is automatically enabled when the **auto ip sla mpls-lsp-monitor** command is entered.
Step 4	**mpls discovery vpn interval** *seconds* **Example:** `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. The default time interval is 300 seconds.
Step 5	**auto ip sla mpls-lsp-monitor** *operation-number* **Example:** `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. **Note** Entering this command automatically enables the **mpls discovery vpn next-hop** command.

Step 6	**type echo** [**saa-vrf-all** | **vrf** *vpn-name*]
	or
	type pathEcho [**saa-vrf-all** | **vrf** *vpn-name*]
	
	Example:
	`Router(config-auto-ip-sla-mpls)# type echo saa-vrf-all`
	or
	
	Example:
	`Router(config-auto-ip-sla-mpls)# type pathEcho saa-vrf-all`
		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.
		or
		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.

Step 7	**access-list** *access-list-number* **Example:** `Router(config-auto-ip-sla-mpls-params)# access-list 10`	(Optional) Specifies the access list to apply to an LSP Health Monitor operation.
Step 8	**scan-interval** *minutes* **Example:** `Router(config-auto-ip-sla-mpls-params)# scan-interval 5`	(Optional) Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates. The default time interval is 240 minutes. At each interval, a new IP SLAs operation is automatically created for each newly discovered BGP next hop neighbor listed in the LSP Health Monitor scan queue.

	Command or Action	Purpose
Step 9	**delete-scan-factor** *factor* **Example:** `Router(config-auto-ip-sla-mpls-params)# delete-scan-factor 2`	(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. The default scan factor is 1. In other words, 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. 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. **Note** This command must be used with the **scan-interval** command.
Step 10	**force-explicit-null** **Example:** `Router(config-auto-ip-sla-mpls-params)# force-explicit-null`	(Optional) Adds an explicit null label to all echo request packets of an IP SLAs operation.
Step 11	**exp** *exp-bits* **Example:** `Router(config-auto-ip-sla-mpls-params)# exp 5`	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation. The default experimental field value is 0.
Step 12	**lsp-selector** *ip-address* **Example:** `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. The default IP address is 127.0.0.0.
Step 13	**reply-dscp-bits** *dscp-value* **Example:** `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. The default DSCP value is 0.
Step 14	**reply-mode** {**ipv4** | **router-alert**} **Example:** `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. The default reply mode is an IPv4 UDP packet.
Step 15	**request-data-size** *bytes* **Example:** `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. For an IP SLAs LSP ping operation, the default is 100 bytes.

	Command or Action	Purpose
Step 16	**secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency* **Example:** `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.
Step 17	**tag** *text* **Example:** `Router(config-auto-ip-sla-mpls-params)# tag testgroup`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	**threshold** *milliseconds* **Example:** `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.
Step 19	**timeout** *milliseconds* **Example:** `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. The default timeout value is 5000 ms. **Note** The default timeout values vary by operation type.
Step 20	**ttl** *time-to-live* **Example:** `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.
Step 21	**exit** **Example:** `Router(config-auto-ip-sla-mpls-params)# exit`	Exits MPLS parameters configuration submode and returns to global configuration mode.
Step 22	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}] **Example:** `Router(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss action-type trapOnly threshold-type consecutive 3`	(Optional) Configures certain actions to occur based on events under the control of the LSP Health Monitor.

	Command or Action	Purpose
Step 23	**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**}] **Example:** `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.
Step 24	**exit** **Example:** `Router(config)# exit`	Exits global configuration submode and returns to privileged EXEC mode.

Manually Configuring an IP SLAs LSP Ping or LSP Traceroute Operation

Perform this task to manually configure an IP SLAs LSP ping or LSP traceroute operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor** *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 monitor 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 monitor logging traps**
15. **ip sla monitor 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla monitor** *operation-number* **Example:** `Router(config)# ip sla monitor 1`	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

Step 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**}}]
	
	Example:
	`Router(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
	or
	
	Example:
	`Router(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
		Configures the IP SLAs operation as an LSP ping operation and enters LSP ping configuration mode.
		or
		Configures the IP SLAs operation as an LSP trace operation and enters LSP trace configuration mode.

Step 5	**exp** *exp-bits* **Example:** `Router(config-sla-monitor-lspPing)# exp 5`	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation. The default experimental field value is 0.
Step 6	**request-data-size** *bytes* **Example:** `Router(config-sla-monitor-lspPing)# request-data-size 200`	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation. For an IP SLAs LSP ping operation, the default is 100 bytes.

	Command or Action	Purpose
Step 7	**secondary-frequency** {**connection-loss** | **timeout**} *frequency* **Example:** `Router(config-sla-monitor-lspPing)# 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.
Step 8	**tag** *text* **Example:** `Router(config-sla-monitor-lspPing)# tag testgroup`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	**threshold** *milliseconds* **Example:** `Router(config-sla-monitor-lspPing)# threshold 6000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 10	**timeout** *milliseconds* **Example:** `Router(config-sla-monitor-lspPing)# timeout 7000`	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet. The default timeout value is 5000 ms. **Note** The default timeout values vary by operation type.
Step 11	**ttl** *time-to-live* **Example:** `Router(config-sla-monitor-lspPing)# ttl 200`	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.
Step 12	**exit** **Example:** `Router(config-sla-monitor-lspPing)# exit`	Exits LSP ping configuration submode and returns to global configuration mode.
Step 13	**ip sla monitor 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**}] **Example:** `Router(config)# ip sla monitor reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type traponly`	(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.
Step 14	**ip sla monitor logging traps** **Example:** `Router(config)# ip sla monitor logging traps`	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.

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

Verifying and Troubleshooting the LSP Health Monitor

Perform this task to verify and troubleshoot the LSP Health Monitor.

SUMMARY STEPS

1. **debug ip sla monitor mpls-lsp-monitor** [*operation-number*]
2. **show ip sla monitor mpls-lsp-monitor configuration** [*operation-number*]
3. **show ip sla monitor mpls-lsp-monitor neighbors**
4. **show ip sla monitor mpls-lsp-monitor scan-queue** *operation-number*
5. **show ip sla monitor statistics** [*operation-number*] [**details**]
6. **show ip sla monitor statistics aggregated** [*operation-number*] [**details**]
7. **show mpls discovery vpn**

DETAILED STEPS

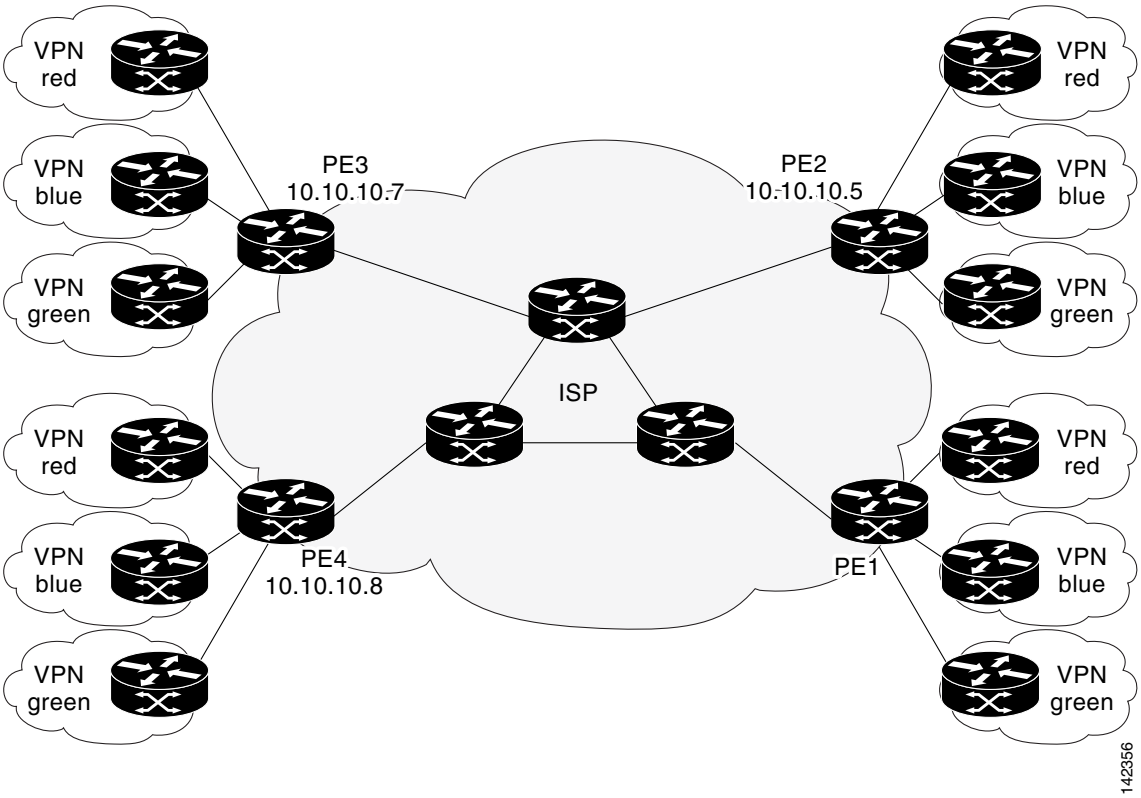
	Command or Action	Purpose
Step 1	**debug ip sla monitor mpls-lsp-monitor** [*operation-number*] **Example:** `Router# debug ip sla monitor mpls-lsp-monitor`	(Optional) Enables debugging output for the LSP Health Monitor.
Step 2	**show ip sla monitor mpls-lsp-monitor configuration** [*operation-number*] **Example:** `Router# show ip sla monitor mpls-lsp-monitor configuration 1`	(Optional) Displays configuration settings for LSP Health Monitor operations.
Step 3	**show ip sla monitor mpls-lsp-monitor neighbors** **Example:** `Router# show ip sla monitor mpls-lsp-monitor neighbors`	(Optional) Displays routing and connectivity information about MPLS VPN BGP next hop neighbors discovered by the LSP Health Monitor.
Step 4	**show ip sla monitor mpls-lsp-monitor scan-queue** *operation-number* **Example:** `Router# show ip sla monitor mpls-lsp-monitor scan-queue 1`	(Optional) Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an LSP Health Monitor operation.
Step 5	**show ip sla monitor statistics** [*operation-number*] [**details**] **Example:** `Router# show ip sla monitor statistics 100001`	(Optional) Displays the current operational status and statistics of all IP SLAs operations or a specified operation. **Note** This command applies only to manually configured IP SLAs operations.
Step 6	**show ip sla monitor statistics aggregated** [*operation-number*] [**details**] **Example:** `Router# show ip sla monitor statistics aggregated 100001`	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation. **Note** This command applies only to manually configured IP SLAs operations.
Step 7	**show mpls discovery vpn** **Example:** `Router# show mpls discovery vpn`	(Optional) Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

Configuration Examples for LSP Health Monitor

Example: Configuring and Verifying the LSP Health Monitor

Figure 2 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).

Figure 2 Network Used for LSP Health Monitor Example



The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options on router PE1 (see Figure 2) 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 saa-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
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type
consecutive 3 action-type trapOnly
!
ip sla monitor logging 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 monitor mpls-lsp-monitor configuration** command for router PE1:

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

Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type      : echo
Vrf Name            : saa-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
```

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

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

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

The following is sample output from the **show ip sla monitor mpls-lsp-monitor scan-queue 1** and **debug ip sla monitor 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 monitor 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


PE1# debug ip sla monitor mpls-lsp-monitor

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

Example: Manually Configuring an IP SLAs LSP Ping Operation

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

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

Additional References

Related Documents

Related Topic	Document Title
MPLS LSP ping and LSP traceroute management tools	*MPLS Embedded Management—Ping/Traceroute and AToM VCCV*, Cisco IOS feature module, Release 12.2(28)SB
Multioperation scheduling for Cisco IOS IP SLAs	"IP SLAs—Multiple Operation Scheduling" chapter of the *IP SLAs Configuration Guide*
Proactive threshold monitoring for Cisco IOS IP SLAs	"IP SLAs—Proactive Threshold Monitoring" chapter of the *IP SLAs Configuration Guide*
Cisco IOS IP SLAs configuration tasks	*Cisco IOS IP SLAs Configuration Guide*, Release 12.4
Cisco IOS IP SLAs commands	*Cisco IOS IP SLAs Command Reference*

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: http://www.cisco.com/go/mibs

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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for the LSP Health Monitor

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for the LSP Health Monitor

Feature Name	Releases	Feature Information
IP SLAs—LSP Health Monitor	12.2(33)SXH	The IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor feature provides the capability to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

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. 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)

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