



IP SLAs—LSP Health Monitor

First Published: February 27, 2006

Last Updated: June 30, 2006

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 Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for the LSP Health Monitor”](#) section on page 83.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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 the LSP Health Monitor, page 2](#)
- [Restrictions for the LSP Health Monitor, page 2](#)
- [Information About the LSP Health Monitor, page 2](#)
- [How to Use the LSP Health Monitor, page 6](#)
- [Configuration Examples for LSP Health Monitor, page 15](#)
- [Additional References, page 19](#)



Corporate Headquarters:

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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 20](#)
- [Feature Information for the LSP Health Monitor, page 83](#)

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 19](#).

**Note**

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

Restrictions for the LSP Health Monitor

- The LSP Health Monitor feature supports only Layer 3 MPLS VPNs.
- The 12.4(6)T and 12.0(32)SY implementation of the LSP Health Monitor supports 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

To use the LSP Health Monitor feature, you should understand the following concepts:

- [Benefits of the LSP Health Monitor, page 2](#)
- [How the LSP Health Monitor Works, page 3](#)
- [Discovery of Neighboring PE Routers, page 4](#)
- [IP SLAs LSP Ping and LSP Traceroute Operations, page 5](#)
- [Proactive Threshold Monitoring for the LSP Health Monitor, page 5](#)
- [Multioperation Scheduling for the LSP Health Monitor, page 6](#)

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 19](#).

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.

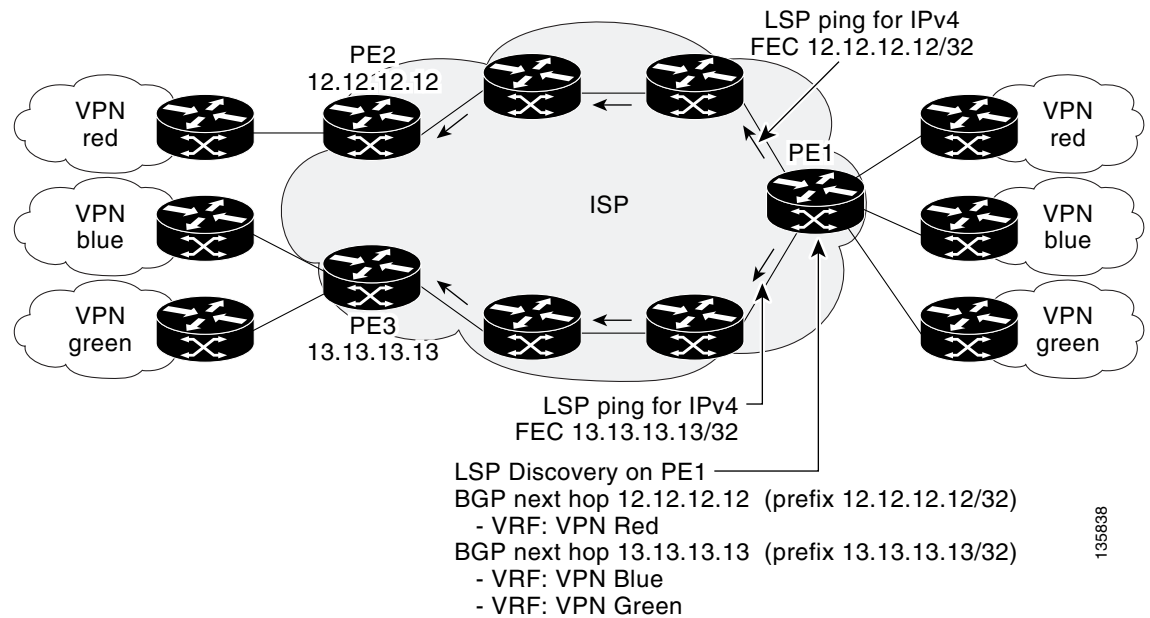
Discovery of Neighboring PE Routers

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 19](#).

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 10.

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 19.

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 19](#).

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 19](#).

How to Use the LSP Health Monitor

This section contains the following tasks:

- [Configuring the LSP Health Monitor on a Source PE Router, page 6](#) (required)
- [Manually Configuring an IP SLAs LSP Ping or LSP Traceroute Operation, page 10](#) (optional)
- [Verifying and Troubleshooting the LSP Health Monitor, page 13](#) (optional)

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** | **pathEcho** } [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. **access-list** *access-list-number*
8. **delete-scan-factor** *factor*
9. **exp** *exp-bits*
10. **force-explicit-null**
11. **lsp-selector** *ip-address*
12. **reply-dscp-bits** *dscp-value*
13. **reply-mode** { **ipv4** | **router-alert** }
14. **request-data-size** *bytes*
15. **scan-interval** *minutes*
16. **secondary-frequency** { **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** *monitored-element* [**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	Enables privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
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 pathEcho} [ipsla-vrf-all vrf vpn-name] Example: Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all	Configures the parameters for an IP SLAs LSP ping or LSP traceroute operation using the LSP Health Monitor. By default, the LSP Health Monitor discovers all BGP next hop neighbors in use by all VRFs associated with the source PE router.
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	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 9	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 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.

	Command or Action	Purpose
Step 11	lsp-selector <i>ip-address</i> 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 127.0.0.1.
Step 12	reply-dscp-bits <i>dscp-value</i> 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 13	reply-mode { <i>ipv4</i> <i>router-alert</i> } 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 14	request-data-size <i>bytes</i> 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.
Step 15	scan-interval <i>minutes</i> 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.
Step 16	secondary-frequency { <i>connection-loss</i> <i>timeout</i> } <i>frequency</i> 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 <i>text</i> Example: Router(config-auto-ip-sla-mpls-params)# tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	threshold <i>milliseconds</i> Example: Router(config-auto-ip-sla-mpls-params)# threshold 6000	(Optional) Specifies the rising threshold (hysteresis) that generates a reaction event and stores history information for the IP SLAs operation. The default threshold value is 5000 ms.

	Command or Action	Purpose
Step 19	timeout <i>milliseconds</i> 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 <i>time-to-live</i> 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 auto IP SLA MPLS configuration submode and returns to global configuration mode.
Step 22	auto ip sla mpls-lsp-monitor reaction-configuration <i>operation-number</i> react <i>monitored-element</i> [action-type <i>option</i>] [threshold-type { consecutive [<i>occurrences</i>] 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.
Step 23	auto ip sla mpls-lsp-monitor schedule <i>operation-number</i> schedule-period <i>seconds</i> [frequency [<i>seconds</i>]] [start-time { after <i>hh:mm:ss</i> <i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] 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** *operation-number*

4. **mpls lsp** {**ping** | **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 schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*month day | day month*] | **pending** | **now** | **after** *hh:mm:ss*}] [**ageout** *seconds*] [**recurring**]
15. **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 <i>operation-number</i> Example: Router(config)# ip sla 1	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	mpls lsp { ping trace } ipv4 <i>destination-address destination-mask</i> [force-explicit-null] [lsp-selector <i>ip-address</i>] [src-ip-addr <i>source-address</i>] [reply { dscp <i>dscp-value</i> 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	Manually configures the parameters for an individual IP SLAs LSP ping or LSP traceroute operation.

	Command or Action	Purpose
Step 5	exp <i>exp-bits</i> Example: Router(config-ip-sla-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 <i>bytes</i> Example: Router(config-ip-sla-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.
Step 7	secondary-frequency { connection-loss timeout } <i>frequency</i> Example: Router(config-ip-sla-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 <i>text</i> Example: Router(config-ip-sla-lspPing)# tag testgroup	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	threshold <i>milliseconds</i> Example: Router(config-ip-sla-lspPing)# threshold 6000	(Optional) Specifies the rising threshold (hysteresis) that generates a reaction event and stores history information for the IP SLAs operation. The default threshold value is 5000 ms.
Step 10	timeout <i>milliseconds</i> Example: Router(config-ip-sla-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 <i>time-to-live</i> Example: Router(config-ip-sla-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-ip-sla-lspPing)# exit	Exits IP SLA configuration submode and returns to global configuration mode.

	Command or Action	Purpose
Step 13	<pre>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}]</pre> Example: <pre>Router(config)# ip sla reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type traponly</pre>	(Optional) Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.
Step 14	<pre>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]</pre> Example: <pre>Router(config)# ip sla schedule 1 start-time now</pre>	Configures the scheduling parameters for an IP SLAs operation.
Step 15	<pre>exit</pre> Example: <pre>Router(config)# exit</pre>	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. `show mpls discovery vpn`
2. `show ip sla mpls-lsp-monitor configuration [operation-number]`
3. `show ip sla mpls-lsp-monitor neighbors`
4. `show ip sla mpls-lsp-monitor scan-queue operation-number`
5. `debug ip sla mpls-lsp-monitor [operation-number]`
6. `show ip sla configuration [operation-number]`
7. `show ip sla statistics [operation-number] [details]`
8. `show ip sla statistics aggregated [operation-number] [details]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	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.
Step 2	show ip sla mpls-lsp-monitor configuration [operation-number] Example: Router# show ip sla mpls-lsp-monitor configuration 1	(Optional) Displays configuration settings for LSP Health Monitor operations.
Step 3	show ip sla mpls-lsp-monitor neighbors Example: Router# show ip sla 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 mpls-lsp-monitor scan-queue operation-number Example: Router# show ip sla 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	debug ip sla mpls-lsp-monitor [operation-number] Example: Router# debug ip sla mpls-lsp-monitor	(Optional) Enables debugging output for the LSP Health Monitor.
Step 6	show ip sla configuration [operation-number] Example: Router# show ip sla configuration 100001	(Optional) Displays configuration settings for IP SLAs operations.
Step 7	show ip sla statistics [operation-number] [details] Example: Router# show ip sla statistics 100001	(Optional) Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
Step 8	show ip sla statistics aggregated [operation-number] [details] Example: Router# show ip sla statistics aggregated 100001	(Optional) Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

Configuration Examples for LSP Health Monitor

This section provides the following configuration examples:

- [Configuring and Verifying the LSP Health Monitor: Example, page 15](#)
- [Manually Configuring an IP SLAs LSP Ping Operation: Example, page 18](#)

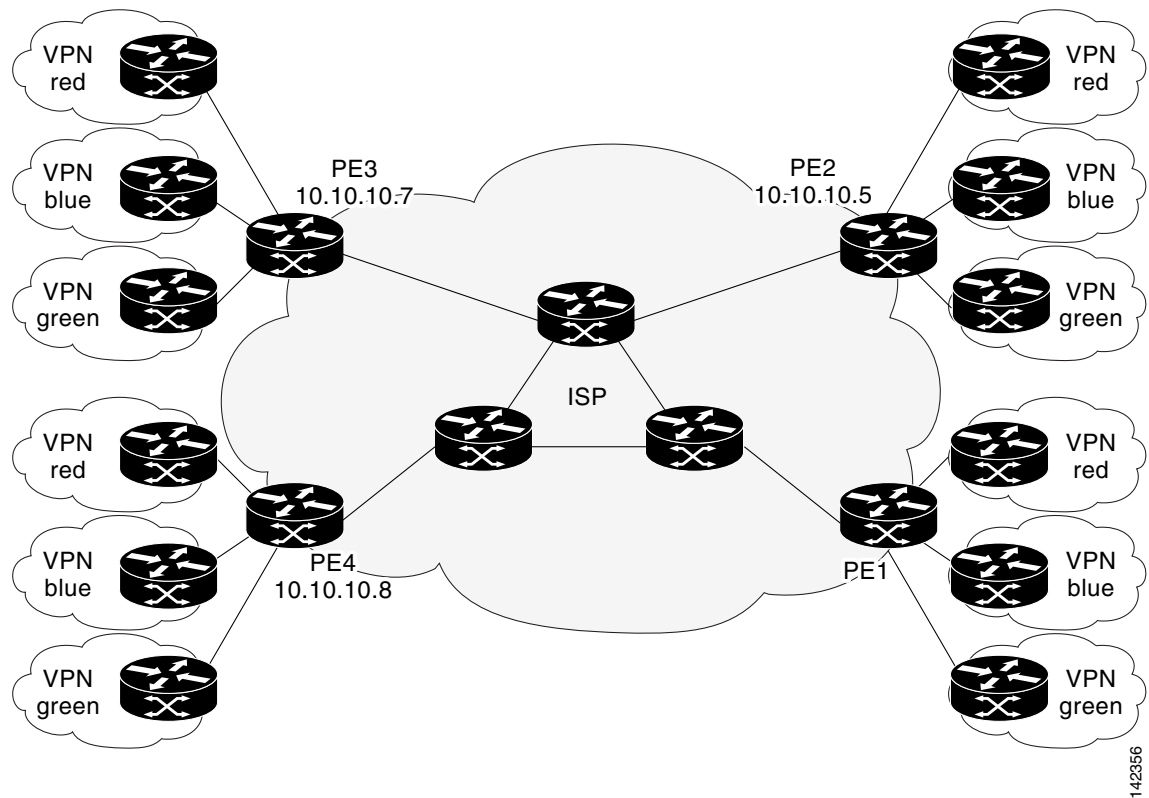
Configuring and Verifying the LSP Health Monitor: Example

[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).

The following example shows how to configure operation parameters, reaction conditions, and scheduling options on router PE1 (see [Figure 2](#)) using the LSP Health Monitor. In this example, LSP Health Monitor 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.

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 connection-loss 10
  secondary-frequency timeout 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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Figure 2 Network Used for LSP Health Monitor Example

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

```

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

```
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
```

Manually Configuring an IP SLAs LSP Ping Operation: Example

The following example shows how to manually configure and schedule an individual 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 connection-loss 30
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
```

Additional References

The following sections provide references related to the LSP Health Monitor feature.

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 12.0(27)S
Configuring standard IP access lists	“ IP Access Lists ” chapter of the <i>Cisco IOS IP Application Services Configuration Guide</i> , Release 12.4
Cisco IOS IP SLAs command line interface enhancements	Cisco IOS IP Service Level Agreements Command Line Interface , Cisco white paper http://www.cisco.com/en/US/products/ps6602/products_white_paper0900aecd8022c2cc.shtml
Multioperation scheduling for Cisco IOS IP SLAs	“ IP SLAs—Multiple Operation Scheduling ” chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> , Release 12.4
Proactive threshold monitoring for Cisco IOS IP SLAs	“ IP SLAs—Proactive Threshold Monitoring ” chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> , Release 12.4
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 , Release 12.4T

Standards

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

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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new commands only.

- [access-list \(IP SLA\)](#)
- [auto ip sla mpls-lsp-monitor](#)
- [auto ip sla mpls-lsp-monitor reaction-configuration](#)
- [auto ip sla mpls-lsp-monitor reset](#)
- [auto ip sla mpls-lsp-monitor schedule](#)
- [debug ip sla mpls-lsp-monitor](#)
- [delete-scan-factor](#)
- [exp \(IP SLA\)](#)
- [force-explicit-null](#)
- [lsp-selector](#)
- [mpls discovery vpn interval](#)
- [mpls discovery vpn next-hop](#)
- [mpls lsp ping ipv4](#)
- [mpls lsp trace ipv4](#)
- [reply-dscp-bits](#)
- [reply-mode](#)
- [scan-interval](#)
- [secondary-frequency](#)
- [show ip sla mpls-lsp-monitor configuration](#)
- [show ip sla mpls-lsp-monitor neighbors](#)

- `show ip sla mpls-lsp-monitor scan-queue`
- `show mpls discovery vpn`
- `ttl (IP SLA)`
- `type echo (MPLS)`
- `type pathEcho (MPLS)`

access-list (IP SLA)

To specify the access list to apply to a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **access-list** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number*

no access-list *access-list-number*

Syntax Description

<i>access-list-number</i>	Number of an access list. This value is a decimal number from 1 to 99 or from 1300 to 1999.
---------------------------	---

Command Default

No access list is specified.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

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 IP SLAs LSP Health Monitor. When the IP SLAs access list parameter is configured, the list of Border Gateway Protocol (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.

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 1](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Table 1 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. Standard IP access list 10 is specified to restrict the number of IP SLAs operations to be created by LSP Health Monitor operation 1. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 1](#)).

Auto IP SLA MPLS Configuration

```
!Configure standard IP access list in global configuration mode
access-list 10 permit 10.10.10.8
!
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 connection-loss 10
  secondary-frequency timeout 10
  access-list 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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
!Configure standard IP access list in global configuration mode
access-list 10 permit 10.10.10.8
!
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  access-list 10
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
```

■ access-list (IP SLA)

```
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

auto ip sla mpls-lsp-monitor

To begin configuration for an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation and enter auto IP SLA Multiprotocol Label Switching (MPLS) configuration mode, use the **auto ip sla mpls-lsp-monitor** command in global configuration mode. To remove all configuration information for an LSP Health Monitor operation, use the **no** form of this command.

auto ip sla mpls-lsp-monitor *operation-number*

no auto ip sla mpls-lsp-monitor *operation-number*

Syntax Description	<i>operation-number</i>	Number used for the identification of the LSP Health Monitor operation you wish to configure.
---------------------------	-------------------------	---

Command Default	No LSP Health Monitor operation is configured.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	Entering this command automatically enables the mpls discovery vpn next-hop command.
	After you configure an LSP Health Monitor operation, you must schedule the operation. To schedule an LSP Health Monitor operation, use the auto ip sla mpls-lsp-monitor schedule command in global configuration mode. You can also optionally set reaction configuration for the operation (see the auto ip sla mpls-lsp-monitor reaction-configuration command).
	To display the current configuration settings of an LSP Health Monitor operation, use the show ip sla mpls-lsp-monitor configuration command in EXEC mode.

Examples	The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router.
-----------------	--

```
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 connection-loss 10
  secondary-frequency timeout 10
!
```

■ auto ip sla mpls-lsp-monitor

```

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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLAs LSP Health Monitor.
auto ip sla mpls-lsp-monitor reset	Removes all IP SLAs LSP Health Monitor configuration from the running configuration.
auto ip sla mpls-lsp-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.
mpls discovery vpn next-hop	Enables the MPLS VPN BGP next hop neighbor discovery process.
show ip sla mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.
type echo (MPLS)	Configures the parameters for a Cisco IOS IP SLAs LSP ping operation using the LSP Health Monitor.
type pathEcho (MPLS)	Configures the parameters for a Cisco IOS IP SLAs LSP traceroute operation using the LSP Health Monitor.

auto ip sla mpls-lsp-monitor reaction-configuration

To configure certain actions to occur based on events under the control of the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor, use the **auto ip sla mpls-lsp-monitor reaction-configuration** command in global configuration mode. To clear all reaction configuration for a specified LSP Health Monitor operation, use the **no** form of this command.

auto ip sla mpls-lsp-monitor reaction-configuration *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** { **consecutive** [*occurrences*] | **immediate** | **never** }]

no auto ip sla mpls-lsp-monitor reaction-configuration *operation-number*

Syntax Description	<i>operation-number</i>	Number of the LSP Health Monitor operation for which reactions are to be configured.
react <i>monitored-element</i>		Specifies the element to be monitored for violations. Keyword options for the monitored element are: • connectionLoss—Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. • timeout—Specifies that a reaction should occur if there is a one-way timeout for the monitored operation.
action-type <i>option</i>		(Optional) Specifies what action or combination of actions the operation performs when threshold events occur. If the threshold-type never keywords are defined, the action-type keyword is disabled. The <i>option</i> argument can be one of the following keywords: • none—No action is taken. This option is the default value. • trapOnly—Send an SNMP logging trap when the specified violation type occurs for the monitored element. IP SLAs logging traps are enabled using the ip sla logging traps command.
threshold-type consecutive <i>[occurrences]</i>		(Optional) When the reaction conditions (such as a timeout) for the monitored element are met consecutively for a specified number of times, perform the action defined by the action-type keyword. The default number of 5 consecutive occurrences can be changed using the <i>occurrences</i> argument. The valid range is from 1 to 16.
threshold-type immediate		(Optional) When the reaction conditions (such as a timeout) for the monitored element are met, immediately perform the action defined by the action-type keyword.
threshold-type never		(Optional) Do not calculate threshold violations. This option is the default threshold type.

Command Default No IP SLAs reactions are generated.

Command Modes Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can configure the **auto ip sla mpls-lsp-monitor reaction-configuration** command multiple times to allow reactions for multiple monitored elements for the same operation. However, disabling of granular reaction elements (for example, entering the **no auto ip sla mpls-lsp-monitor reaction-configuration operation-number react monitored-element** command) is not supported. To clear all reaction configuration for a particular LSP Health Monitor operation, use the **no auto ip sla mpls-lsp-monitor reaction-configuration operation-number** command.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. The **ip sla logging traps** command is used to enable the generation of SNMP traps specific to IP SLAs threshold violations.

**Note**

Keywords are not case sensitive and are shown in mixed case for readability only.

To display the current configuration settings of an LSP Health Monitor operation, use the **show ip sla mpls-lsp-monitor configuration** command in EXEC mode.

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified by the reaction condition configuration, when three consecutive connection loss or timeout events occur, an SNMP logging trap is sent.

```
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 connection-loss 10
  secondary-frequency timeout 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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
show ip sla mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.

auto ip sla mpls-lsp-monitor reset

To remove all IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor configuration from the running configuration, use the **auto ip sla mpls-lsp-monitor reset** command in global configuration mode.

auto ip sla mpls-lsp-monitor reset

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	To clear IP SLAs configuration information (not including IP SLAs LSP Health Monitor configuration) from the running configuration, use the ip sla reset command in global configuration mode.
-------------------------	---

Examples	The following example shows how to remove all the LSP Health Monitor configurations from the running configuration:
-----------------	---

```
auto ip sla mpls-lsp-monitor reset
```

Related Commands	Command	Description
	ip sla reset	Stops all IP SLAs operations, clears IP SLAs configuration information, and returns the IP SLAs feature to the startup condition.

auto ip sla mpls-lsp-monitor schedule

To configure the scheduling parameters for an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **auto ip sla mpls-lsp-monitor schedule** command in global configuration mode. To stop the operation and place it in the default state (pending), use the **no** form of this command.

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** }]

no auto ip sla mpls-lsp-monitor schedule *operation-number*

Syntax Description

<i>operation-number</i>	Number of the LSP Health Monitor operation to be scheduled.
schedule-period <i>seconds</i>	Specifies the amount of time (in seconds) for which the LSP Health Monitor is scheduled.
frequency <i>seconds</i>	(Optional) Specifies the number of seconds after which each IP SLAs operation is restarted. The default frequency is the value specified for the schedule period.
start-time	(Optional) Time when the operation starts collecting information. If the start time is not specified, no information is collected.
after <i>hh:mm:ss</i>	(Optional) Indicates that the operation should start <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after this command was entered.
<i>hh:mm[:ss]</i>	(Optional) Specifies an absolute start time using hours, minutes, and seconds. Use the 24-hour clock notation. For example, start-time 01:02 means “start at 1:02 a.m.,” and start-time 13:01:30 means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a month and day.
<i>month</i>	(Optional) Name of the month in which to start the operation. If a month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month.
<i>day</i>	(Optional) Number of the day (in the range 1 to 31) on which to start the operation. If a day is not specified, the current day is used. Use of this argument requires that a month be specified.
now	(Optional) Indicates that the operation should start immediately.
pending	(Optional) No information is collected. This option is the default value.

Command Default

The LSP Health Monitor operation is placed in a pending state (that is, the operation is enabled but is not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

After you schedule an LSP Health Monitor operation with the **auto ip sla mpls-lsp-monitor schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no auto ip sla mpls-lsp-monitor operation-number** command in global configuration mode and then enter the new configuration information.

To display the current configuration settings of an LSP Health Monitor operation, use the **show ip sla mpls-lsp-monitor configuration** command in user EXEC or privileged EXEC mode.

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified in the example configuration, the schedule period for LSP Health Monitor operation 1 is 60 seconds and the operation is scheduled to start immediately.

```
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 connection-loss 10
  secondary-frequency timeout 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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
show ip sla mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.

debug ip sla mpls-lsp-monitor

To enable debugging output for the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor, use the **debug ip sla mpls-lsp-monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip sla mpls-lsp-monitor [*operation-number*]

no debug ip sla mpls-lsp-monitor [*operation-number*]

Syntax Description	<i>operation-number</i> (Optional) Number of the LSP Health Monitor operation for which the debugging output will be displayed.	
Command Default	Debug is not enabled.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.4(6)T	This command was introduced.

Examples

The following is sample output from the **debug ip sla mpls-lsp-monitor** command. This output shows that three VPNs associated with router 10.10.10.8 (red, blue, and green) were discovered and that this information was added to the LSP Health Monitor scan queue. Also, since router 10.10.10.8 is a newly discovered Border Gateway Protocol (BGP) next hop neighbor, a new IP SLAs operation for router 10.10.10.8 (Probe 100005) is being created and added to the LSP Health Monitor multioperation schedule. Even though router 10.10.10.8 belongs to three VPNs, only one IP SLAs operation is being created.

Router# **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
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.

delete-scan-factor

To specify the number of times the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor should check the scan queue before automatically deleting IP SLAs operations for Border Gateway Protocol (BGP) next hop neighbors that are no longer valid, use the **delete-scan-factor** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To return to the default value, use the **no** form of this command.

delete-scan-factor *factor*

no delete-scan-factor

Syntax Description

<i>factor</i>	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.
---------------	--

Command Default

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.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

This command must be used with the **scan-interval** command. Use the **scan-interval** command in IP SLA monitor configuration mode to specify the time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.



Note

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.

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 2](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Table 2 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. The delete scan factor is set to 2. In other words, every other 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. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 2](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
```

■ delete-scan-factor

```

rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.
scan-interval	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.
show ip sla mpls-lsp-monitor scan-queue	Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an IP SLAs LSP Health Monitor operation.
show rtr mpls-lsp-monitor scan-queue	Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an IP SLAs LSP Health Monitor operation.

exp (IP SLA)

To specify the experimental field value in the header for an echo request packet of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **exp** command in the appropriate submode of auto IP SLA MPLS configuration, IP SLA configuration, SAA MPLS configuration, or RTR configuration mode. To return to the default value, use the **no** form of this command.

exp *exp-bits*

no exp

Syntax Description

<i>exp-bits</i>	Specifies the experimental field value in the header for an echo request packet. Valid values are from 0 to 7. Default is 0.
-----------------	--

Command Default

The experimental field value is set to 0.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

IP SLA Configuration

LSP ping configuration (config-sla-monitor-lspPing)

LSP trace configuration (config-sla-monitor-lspTrace)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)

RTR Configuration

LSP ping configuration (config-rtr-lspPing)

LSP trace configuration (config-rtr-lspTrace)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines**IP SLAs Operation Configuration Dependence on Cisco IOS Release**

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 3](#)). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see [Table 4](#) for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation.

The configuration mode for the **exp** (IP SLA) command varies depending on the Cisco IOS release you are running and the operation type configured. For example, if you are running Cisco IOS Release 12.4(6)T and the LSP ping operation type is configured (without using the LSP Health Monitor), you would enter the **exp** (IP SLA) command in LSP ping configuration mode (config-sla-monitor-lspPing) within IP SLA configuration mode.

Table 3 *Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release*

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T or later releases	ip sla	IP SLA configuration
All other Cisco IOS releases	rtr	RTR configuration

Table 4 *Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release*

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. The experimental field value for each IP SLAs operations created by LSP Health Monitor operation 1 is set to 5. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 4](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  exp 5
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

SAA MPLS Configuration

```

mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  exp 5
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

force-explicit-null

To add an explicit null label to all echo request packets of a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **force-explicit-null** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To return to the default value, use the **no** form of this command.

force-explicit-null

no force-explicit-null

Syntax Description

This command has no arguments or keywords.

Command Default

An explicit null label is not added.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 5](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Table 5 *Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release*

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source PE router. As specified in the example configuration, an explicit null label be added to all the echo request packets of IP SLAs operations created by LSP Health Monitor operation 1. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 5](#)).

Auto IP SLA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
  type echo ipsla-vrf-all
  force-explicit-null
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  force-explicit-null
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

lsp-selector

To specify the local host IP address used to select the label switched path (LSP) for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **lsp-selector** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To return to the default value, use the **no** form of this command.

lsp-selector *ip-address*

no lsp-selector *ip-address*

Syntax Description

<i>ip-address</i>	Specifies a local host IP address used to select the LSP.
-------------------	---

Command Default

The local host IP address used to select the LSP is 127.0.0.1.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

This command is used to force an IP SLAs operation to use a specific LSP to obtain its response time measurement. This option is useful if there are multiple equal cost paths between Provider Edge (PE) routers.

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 6](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Table 6 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source PE router. As specified in the example configuration, IP address 127.0.0.1 is the local host IP address chosen to select the LSP for obtaining response time measurements. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 6](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  lsp-selector 127.0.0.10
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  lsp-selector 127.0.0.10
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
```

```

rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

mpls discovery vpn interval

To specify the time interval at which routing entries that are no longer valid are removed from the Border Gateway Protocol (BGP) next hop neighbor discovery database of a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN), use the **mpls discovery vpn interval** command in global configuration mode. To return to the default scan interval, use the **no** form of this command.

mpls discovery vpn interval *seconds*

no mpls discovery vpn interval

Syntax Description	<i>seconds</i>	Specifies the time interval (in seconds) at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
---------------------------	----------------	--

Command Default	The default time interval is 300 seconds.
------------------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines	When the BGP next hop neighbor discovery process is enabled (using the mpls discovery vpn next-hop command), 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 (using the mpls discovery vpn interval command).
-------------------------	---

The BGP next hop neighbor discovery process is used by the Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor feature.

Examples	The following example shows how to enable the MPLS VPN BGP next hop neighbor discovery process and specify 60 seconds as 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:
-----------------	---

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
```

Related Commands

Command	Description
mpls discovery vpn next-hop	Enables the MPLS VPN BGP next hop neighbor discovery process.
show mpls discovery vpn	Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

mpls discovery vpn next-hop

To enable the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Border Gateway Protocol (BGP) next hop neighbor discovery process, use the **mpls discovery vpn next-hop** command in global configuration mode. To disable the discovery process, use the **no** form of this command.

mpls discovery vpn next-hop

no mpls discovery vpn next-hop

Syntax Description This command has no arguments or keywords.

Command Default The BGP next hop neighbor discovery process is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines 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 (using the **mpls discovery vpn interval** command in global configuration mode).

The **mpls discovery vpn next-hop** command is automatically enabled when an IP Service Level Agreements (SLAs) LSP Health Monitor operation is enabled. However, to disable the BGP next hop neighbor discovery process, you must use the **no** form of this command.

Examples The following example shows how to enable the MPLS VPN BGP next hop neighbor discovery process and specify 60 seconds as 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:

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
```

Related Commands

Command	Description
mpls discovery vpn interval	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.
show mpls discovery vpn	Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

mpls lsp ping ipv4

To manually configure an individual Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) ping IPv4 operation, use the **mpls lsp ping ipv4** command in IP SLA configuration mode.

```
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}}]
```

Syntax Description	
<i>destination-address</i>	Address prefix of the target to be tested.
<i>destination-mask</i>	Number of bits in the network mask of the target address.
force-explicit-null	(Optional) Adds an explicit null label to all echo request packets.
lsp-selector <i>ip-address</i>	(Optional) Specifies a local host IP address used to select the LSP. Default address is 127.0.0.1
src-ip-addr <i>source-address</i>	(Optional) Specifies a source IP address for the echo request originator.
reply dscp <i>dscp-value</i>	(Optional) Specifies the differentiated services codepoint (DSCP) value of an echo reply packet. Default DSCP value is 0.
reply mode	(Optional) Specifies the reply mode for the echo request packet.
ipv4	(Optional) Replies with an IPv4 UDP packet (default).
router-alert	(Optional) Replies with an IPv4 UDP packet with router alert.

Command Default No IP SLAs operation type is configured for the operation being configured.

Command Modes IP SLA configuration

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla** global configuration command) and then reconfigure the operation with the new operation type.

The **lsp-selector** keyword is used to force an IP SLAs operation to use a specific LSP to obtain its response time measurement. This option is useful if there are multiple equal cost paths between Provider Edge (PE) routers.

Examples

The following example shows how to manually configure operation parameters, reaction conditions, and scheduling options for IP SLAs LSP ping operation 1:

```
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 connection-loss 30
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
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

mpls lsp trace ipv4

To manually configure an individual Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) traceroute IPv4 operation, use the **mpls lsp trace ipv4** command in IP SLA configuration mode.

```
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}}]
```

Syntax Description	
<i>destination-address</i>	Address prefix of the target to be tested.
<i>destination-mask</i>	Number of bits in the network mask of the target address.
force-explicit-null	(Optional) Adds an explicit null label to all echo request packets.
lsp-selector <i>ip-address</i>	(Optional) Specifies a local host IP address used to select the LSP. Default address is 127.0.0.1.
src-ip-addr <i>source-address</i>	(Optional) Specifies a source IP address for the echo request originator.
reply dscp <i>dscp-value</i>	(Optional) Specifies the differentiated services codepoint (DSCP) value of an echo reply. Default DSCP value is 0.
reply mode	(Optional) Specifies the reply mode for the echo request packet.
ipv4	(Optional) Replies with an IPv4 UDP packet (default).
router-alert	(Optional) Replies with an IPv4 UDP packet with router alert.

Command Default No IP SLAs operation type is configured for the operation being configured.

Command Modes IP SLA configuration

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines You must configure the type of IP SLAs operation (such as LSP trace) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla** global configuration command) and then reconfigure the operation with the new operation type.



Note

This command supports only single path connectivity measurements between the source PE router and associated BGP next hop neighbors.

The **lsp-selector** keyword is used to force an IP SLAs operation to use a specific LSP to obtain its response time measurement. This option is useful if there are multiple equal cost paths between provider edge (PE) routers.

Examples

The following example shows how to manually configure operation parameters, reaction conditions, and scheduling options for IP SLAs LSP traceroute operation 1:

```
ip sla 1
mpls lsp trace 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 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
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

reply-dscp-bits

To specify the differentiated services codepoint (DSCP) value for an echo reply packet of a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **reply-dscp-bits** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To return to the default value, use the **no** form of this command.

reply-dscp-bits *dscp-value*

no reply-dscp-bits *dscp-value*

Syntax Description	<i>dscp-value</i>	Specifies the differentiated services codepoint (DSCP) value for an echo reply packet.
---------------------------	-------------------	--

Command Default	The DSCP value is 0.
------------------------	----------------------

Command Modes	Auto IP SLA MPLS Configuration
	MPLS parameters configuration (config-auto-ip-sla-mpls-params)
	SAA MPLS Configuration
	MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines	IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see Table 7). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.
-------------------------	--

Table 7 *Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release*

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. The DSCP value for the echo reply packets of IP SLAs operations created by LSP Health Monitor operation 1 is set to 5. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 7](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  reply-dscp-bits 5
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  reply-dscp-bits 5
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
```

```
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

reply-mode

To specify the reply mode for an echo request packet of a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **reply-mode** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To return to the default value, use the **no** form of this command.

reply-mode {ipv4 | router-alert}

no reply-mode {ipv4 | router-alert}

Syntax Description

ipv4	Replies with an IPv4 User Datagram Protocol (UDP) packet (default).
router-alert	Replies with an IPv4 UDP packet with router alert.

Command Default

The reply mode for an echo request packet is an IPv4 UDP packet by default.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 8](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Table 8 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified in the example configuration, the reply mode of an echo request packet for IP SLAs operations created by LSP Health Monitor operation 1 is an IPv4 UDP packet with router alert. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 8](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  reply-mode router-alert
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  reply-mode router-alert
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
```

```
rtr logging traps
!  
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

scan-interval

To specify the time interval at which the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor checks the scan queue for BGP next hop neighbor updates, use the **scan-interval** command in the Multiprotocol Label Switching (MPLS) parameters submode of auto IP SLA MPLS configuration or SAA MPLS configuration mode. To return to the default value, use the **no** form of this command.

scan-interval *minutes*

no scan-interval

Syntax Description	<i>minutes</i>	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.
---------------------------	----------------	---

Command Default	Scan interval is 240 minutes.
------------------------	-------------------------------

Command Modes	Auto IP SLA MPLS Configuration
	MPLS parameters configuration (config-auto-ip-sla-mpls-params)
	SAA MPLS Configuration
	MPLS parameters configuration (config-saa-mpls-params)



Note

The configuration mode varies depending on the Cisco IOS release you are running. See the “Usage Guidelines” section for more information.

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines	At each scan interval, a new IP SLA operation is automatically created for each newly discovered BGP next hop neighbor listed in the LSP Health Monitor scan queue. If there is more than one IP SLAs operation created at a specific scan interval, the start time for each newly created IP SLAs operation is randomly distributed to avoid having all of the operations start at the same time. Use the delete-scan-factor command in IP SLA monitor configuration mode to specify 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.
-------------------------	---

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 9](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Table 9 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified in the example configuration, the time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 9](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
```

```

rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
delete-scan-factor	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.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.
show ip sla mpls-lsp-monitor scan-queue	Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an IP SLAs LSP Health Monitor operation.
show rtr mpls-lsp-monitor scan-queue	Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an IP SLAs LSP Health Monitor operation.

secondary-frequency

To set a faster measurement frequency (secondary frequency) to which a Cisco IOS IP Service Level Agreements (SLAs) operation should change when a reaction condition occurs, use the **secondary-frequency** command in the appropriate submode of auto IP SLA MPLS configuration, IP SLA configuration, SAA MPLS configuration, or RTR configuration mode. To disable the secondary frequency, use the **no** form of this command.

secondary-frequency { **both** | **connection-loss** | **timeout** } *frequency*

no secondary-frequency { **connection-loss** | **timeout** }

Syntax Description

both	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way connection loss or one-way timeout is detected.
connection-loss	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way connection loss is detected.
timeout	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way timeout is detected.
<i>frequency</i>	Sets the secondary frequency to which an IP SLAs operation should change when a reaction condition occurs.

Command Default

The secondary frequency option is disabled.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

IP SLA Configuration

LSP ping configuration (config-sla-monitor-lspPing)

LSP trace configuration (config-sla-monitor-lspTrace)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)

RTR Configuration

LSP ping configuration (config-rtr-lspPing)

LSP trace configuration (config-rtr-lspTrace)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

This command provides the capability to specify a secondary frequency for an IP SLAs operation. If the secondary frequency option is configured and a failure (such as a connection loss or timeout) is detected for a particular label-switched path (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.

**Note**

If the secondary frequency option is not enabled, the frequency at which an operation remeasures a failed LSP is the same as the schedule period by default.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 10](#)). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see [Table 11](#) for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation.

The configuration mode for the **secondary-frequency** command varies depending on the Cisco IOS release you are running and the operation type configured. For example, if you are running Cisco IOS Release 12.4(6)T and the LSP ping operation type is configured (without using the LSP Health Monitor), you would enter the **secondary-frequency** command in LSP ping configuration mode (config-sla-monitor-lspPing) within IP SLA configuration mode.

Table 10 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T or later releases	ip sla	IP SLA configuration
All other Cisco IOS releases	rtr	RTR configuration

Table 11 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use

by all VRFs associated with the source Provider Edge (PE) router. The secondary frequency option is enabled for both connection loss and timeout events, and the secondary frequency is set to 10 seconds. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 11](#)).

Auto IP SLA MPLS 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
  delete-scan-factor 2
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency both 10
  delete-scan-factor 2
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

show ip sla mpls-lsp-monitor configuration

To display configuration settings for IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operations, use the **show ip sla mpls-lsp-monitor configuration** command in user EXEC or privileged EXEC mode.

show ip sla mpls-lsp-monitor configuration [*operation-number*]

Syntax Description	<i>operation-number</i>	(Optional) Number of the LSP Health Monitor operation for which the details will be displayed.
---------------------------	-------------------------	--

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Usage Guidelines	If the identification number of an LSP Health Monitor operation is not specified, configuration values for all the configured LSP Health Monitor operations will be displayed.
-------------------------	--

Examples	The following is sample output from the show ip sla mpls-lsp-monitor configuration command:
-----------------	--

```
Router# 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

```

Table 12 describes the significant fields shown in the display.

Table 12 *show ip sla mpls-lsp-monitor configuration Field Descriptions*

Field	Description
Entry Number	Identification number for the LSP Health Monitor operation.
Operation Type	Type of IP SLAs operation configured by the LSP Health Monitor operation.
Vrf Name	If a specific name is displayed in this field, then the LSP Health Monitor is configured to discover only those BGP next hop neighbors in use by the VRF specified. If saa-vrf-all is displayed in this field, then the LSP Health Monitor is configured to discover all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router.
Tag	User-specified identifier for the LSP Health Monitor operation.
EXP Value	Experimental field value in the header for an echo request packet of the IP SLAs operation.
Timeout(ms)	Amount of time the IP SLAs operation waits for a response from its request packet.
Threshold(ms)	Threshold value of the IP SLAs operation for which a reaction event is generated if violated.
Frequency(sec)	Time after which the IP SLAs operation is restarted.
LSP Selector	Local host IP address used to select the LSP for the IP SLAs operation.
ScanInterval(min)	Time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.
Delete Scan Factor	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.
Operations List	Identification numbers IP SLAs operations created by the LSP Health Monitor operation.
Schedule Period(sec)	Amount of time for which the LSP Health Monitor operation is scheduled.
Request size	Protocol data size for the request packet of the IP SLAs operation.
Start Time	Status of the start time for the LSP Health Monitor operation.
SNMP RowStatus	Indicates whether SNMP RowStatus is active or inactive.

Table 12 *show ip sla mpls-lsp-monitor configuration Field Descriptions (continued)*

Field	Description
TTL value	The maximum hop count for an echo request packet of the IP SLAs operation.
Reply Mode	Reply mode for an echo request packet of the IP SLAs operation.
Reply Dscp Bits	Differentiated services codepoint (DSCP) value of an echo reply packet of the IP SLAs operation.
Secondary Frequency	Reaction condition that will enable the secondary frequency option.
Value(sec)	Secondary frequency value.
Reaction Configs	Reaction configuration of the IP SLAs operation.
Reaction	Reaction condition being monitored.
Threshold Type	Specifies when an action should be performed as a result of a reaction event.
Threshold Count	The number of times a reaction event can occur before an action should be performed.
Action Type	Type of action that should be performed as a result of a reaction event.

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
auto ip sla mpls-lsp-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.

show ip sla mpls-lsp-monitor neighbors

To display routing and connectivity information about Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Border Gateway Protocol (BGP) next hop neighbors discovered by the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor, use the **show ip sla mpls-lsp-monitor neighbors** command in user EXEC or privileged EXEC mode.

show ip sla mpls-lsp-monitor neighbors

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.4(6)T	This command was introduced.

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

```
Router# 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)
```

[Table 13](#) describes the significant fields shown in the display.

Table 13 *show ip sla mpls-lsp-monitor neighbors Field Descriptions*

Field	Description
BGP Next hop	Identifier for the BGP next hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.

Table 13 *show ip sla mpls-lsp-monitor neighbors Field Descriptions (continued)*

Field	Description
ProbeID	The identification number of the IP SLAs operation. The names of the VRFs that contain routing entries for the specified BGP next hop neighbor are listed in parentheses.
OK	LSP ping or LSP traceroute connectivity status between the source PE router and specified BGP next hop neighbor. Connectivity status can be the following: • OK—Successful reply. • ConnectionLoss—Reply is from a device that is not egress for the Forward Equivalence Class (FEC). • Timeout—Echo request timeout. • Unknown—State of LSP is not known.

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.

show ip sla mpls-lsp-monitor scan-queue

To display information about adding or deleting Border Gateway Protocol (BGP) next hop neighbors from a particular Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) of an IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **show ip sla mpls-lsp-monitor scan-queue** command in user EXEC or privileged EXEC mode.

show ip sla mpls-lsp-monitor scan-queue *operation-number*

Syntax Description	<i>operation-number</i>	Number of the LSP Health Monitor operation for which the details will be displayed.
--------------------	-------------------------	---

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.4(6)T	This command was introduced.

Examples The following is sample output from the **show ip sla mpls-lsp-monitor scan-queue** command:

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

```
Next scan Time after: 23 Secs
```

```
Next Delete scan Time after: 83 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

[Table 14](#) describes the significant fields shown in the display.

Table 14 *show ip sla mpls-lsp-monitor scan-queue* Field Descriptions

Field	Description
Next scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about adding BGP next hop neighbors to a particular VPN. At the start of each scan time, IP SLAs operations are created for all newly discovered neighbors.
Next Delete scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about deleting BGP next hop neighbors from a particular VPN. At the start of each delete scan time, IP SLAs operations are deleted for neighbors that are no longer valid.
BGP Next hop	Identifier for the BGP next hop neighbor.

Table 14 *show ip sla mpls-lsp-monitor scan-queue Field Descriptions (continued)*

Field	Description
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
vrf	Name of the VRF that contains a routing entry for the specified BGP next hop neighbor.
Add/Delete	Indicates that the specified BGP next hop neighbor will be added to or removed from the specified VPN.

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
delete-scan-factor	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.
mpls discovery vpn interval	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.
scan-interval	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.

show mpls discovery vpn

To display routing information relating to the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Border Gateway Protocol (BGP) next hop neighbor discovery process, use the **show mpls discovery vpn** command in user EXEC or privileged EXEC mode.

show mpls discovery vpn

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Examples The following is sample output from the **show mpls discovery vpn** command:

```
Router# 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
```

Table 15 describes the fields shown in the display.

Table 15 *show mpls discovery vpn Field Descriptions*

Field	Description
Refresh interval	The time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database. The default time interval is 300 seconds.
Next refresh	The amount of time left before the next refresh interval starts.
Next hop	Identifier for the BGP next hop neighbor.

Table 15 *show mpls discovery vpn Field Descriptions (continued)*

Field	Description
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
in use by	Names of the VRFs that contain routing entries for the specified BGP next hop neighbor.

Related Commands

Command	Description
mpls discovery vpn interval	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.
mpls discovery vpn next-hop	Enables the MPLS VPN BGP next hop neighbor discovery process.

ttl (IP SLA)

To specify the maximum hop count for an echo request packet of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **ttl** command in the appropriate submode of auto IP SLA MPLS configuration, IP SLA configuration, SAA MPLS configuration, or RTR configuration mode. To return to the default value, use the **no** form of this command.

ttl *time-to-live*

no ttl

Syntax Description

<i>time-to-live</i>	Specifies the maximum hop count for an echo request packet. For information about valid value ranges and defaults, see the “Usage Guidelines” section for more information.
---------------------	---

Command Default

For IP SLAs LSP ping operations, the default time-to-live value is 255.
For IP SLAs LSP traceroute operations, the default time-to-live value is 30.

Command Modes

Auto IP SLA MPLS Configuration

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

IP SLA Configuration

LSP ping configuration (config-sla-monitor-lspPing)

LSP trace configuration (config-sla-monitor-lspTrace)

SAA MPLS Configuration

MPLS parameters configuration (config-saa-mpls-params)

RTR Configuration

LSP ping configuration (config-rtr-lspPing)

LSP trace configuration (config-rtr-lspTrace)



Note

The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

For IP SLAs LSP ping operations, valid values are from 1 to 255 and the default is 255.

For IP SLAs LSP traceroute operations, valid values are from 1 to 30 and the default is 30.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see [Table 16](#)). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see [Table 17](#) for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation.

The configuration mode for the **ttl** command varies depending on the Cisco IOS release you are running and the operation type configured. For example, if you are running Cisco IOS Release 12.4(6)T and the LSP ping operation type is configured (without using the LSP Health Monitor), you would enter the **ttl** command in LSP ping configuration mode (config-sla-monitor-lspPing) within IP SLA configuration mode.

Table 16 Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T or later releases	ip sla	IP SLA configuration
All other Cisco IOS releases	rtr	RTR configuration

Table 17 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified in the example configuration, the maximum hop count for echo request packets of IP SLAs operations created by LSP Health Monitor operation 1 is 200 hops. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 17](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  ttl 200
!
```

```

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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

SAA MPLS Configuration

```

mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
  ttl 200
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

type echo (MPLS)

To configure Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) ping operations using the LSP Health Monitor, use the **type echo** command in auto IP SLA Multiprotocol Label Switching (MPLS) configuration or SAA MPLS configuration mode.

Auto IP SLA MPLS Configuration

type echo [**ipsla-vrf-all** | **vrf** *vpn-name*]

SAA MPLS Configuration

type echo [**saa-vrf-all** | **vrf** *vpn-name*]

Syntax Description		
	ipsla-vrf-all	(Optional) Specifies that LSP ping operations should be automatically created for all BGP next hop neighbors in use by a VRF corresponding to all the VPNs in which the originating Provider Edge (PE) router belongs. This option is the default.
	vrf <i>vpn-name</i>	(Optional) Specifies that LSP ping operations should be automatically created for only those BGP next hop neighbors associated with the specified VPN name.
	saa-vrf-all	(Optional) Specifies that LSP ping operations should be automatically created for all BGP next hop neighbors in use by a VRF corresponding to all the VPNs in which the originating Provider Edge (PE) router belongs. This option is the default.

Command Default	No IP SLAs operation type is configured for the operation being configured.
-----------------	---

Command Modes	Auto IP SLA MPLS configuration SAA MPLS configuration
---------------	--

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines



Note

When an IP SLAs LSP ping operation is created by the LSP Health Monitor, an operation number (identification number) is automatically assigned to the operation. The operation numbering starts at 100001.

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 18](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no auto ip sla mpls-lsp-monitor** or **no rtr mpls-lsp-monitor** global configuration command) and then reconfigure the operation with the new operation type.

Table 18 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source PE router. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 18](#)).

Auto IP SLA MPLS 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 connection-loss 10
  secondary-frequency timeout 10
  delete-scan-factor 2
!
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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
  type echo saa-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 10
```

```
delete-scan-factor 2
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

type pathEcho (MPLS)

To configure Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) LSP traceroute operations using the LSP Health Monitor, use the **type pathEcho** command in auto IP SLA Multiprotocol Label Switching (MPLS) configuration or SAA MPLS configuration mode. To remove or replace the configuration for an LSP Health Monitor operation, use the **no rtr mpls-lsp-monitor operation-number** global configuration command.

Auto IP SLA MPLS Configuration

type pathEcho [**ipsla-vrf-all** | **vrf** *vpn-name*]

SAA MPLS Configuration

type pathEcho [**saa-vrf-all** | **vrf** *vpn-name*]

Syntax Description		
	ipsla-vrf-all	(Optional) Specifies that LSP traceroute operations should be automatically created for all BGP next hop neighbors in use by a VRF corresponding to all the VPNs in which the originating Provider Edge (PE) router belongs. This option is the default.
	vrf <i>vpn-name</i>	(Optional) Specifies that LSP traceroute operations should be automatically created for only those BGP next hop neighbors associated with the specified VPN name.
	saa-vrf-all	(Optional) Specifies that LSP traceroute operations should be automatically created for all BGP next hop neighbors in use by a VRF corresponding to all the VPNs in which the originating Provider Edge (PE) router belongs. This option is the default.

Command Default	No IP SLAs operation type is configured for the operation being configured.
-----------------	---

Command Modes	Auto IP SLA MPLS configuration SAA MPLS configuration
---------------	--

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines



Note

When an IP SLAs LSP traceroute operation is created by the LSP Health Monitor, an operation number (identification number) is automatically assigned to the operation. The operation numbering starts at 100001.

**Note**

This command supports only single path connectivity measurements between the source PE router and associated BGP next hop neighbors.

IP SLAs LSP Health Monitor Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 19](#)). You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no auto ip sla mpls-lsp-monitor** or **no rtr mpls-lsp-monitor** global configuration command) and then reconfigure the operation with the new operation type.

Table 19 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration
12.2(27)SBC and 12.2(28)SB	rtr mpls-lsp-monitor	SAA MPLS configuration

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP traceroute operations for all BGP next hop neighbors in use by all VRFs associated with the source PE router. Note that the Cisco IOS command used to begin configuration for an IP SLAs LSP Health Monitor operation varies depending on the Cisco IOS release you are running (see [Table 19](#)).

Auto IP SLA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
  type pathEcho ipsla-vrf-all
  timeout 1000
  scan-interval 1
  secondary-frequency connection-loss 10
  secondary-frequency timeout 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 logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

SAA MPLS Configuration

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
```

■ type pathEcho (MPLS)

```

type pathEcho saa-vrf-all
timeout 1000
scan-interval 1
secondary-frequency connection-loss 10
secondary-frequency timeout 10
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now

```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.

Feature Information for the LSP Health Monitor

Table 20 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 20 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 20 Feature Information for the LSP Health Monitor

Feature Name	Releases	Feature Information
IP SLAs—LSP Health Monitor	12.2(27)SBC	The IP SLAs LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs.
IP SLAs—LSP Health Monitor	12.4(6)T, 12.0(32)SY	The IP SLAs LSP Health Monitor feature was integrated into Cisco IOS Release 12.4(6)T and 12.0(32)SY with several enhancements to the command line interface (CLI).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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.

© 2006 Cisco Systems, Inc. All rights reserved.

