IP SLAs—LSP Health Monitor with LSP Discovery

First Published: February 27, 2007
Last Updated: February 27, 2007

The Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor with LSP Discovery feature provides the capability to proactively monitor Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides automated end-to-end verification in the control plane and data plane for all LSPs between the participating Provider Edge (PE) routers. This end-to-end (PE-to-PE router) approach ensures that LSP connectivity is verified along the paths that customer traffic is sent. Consequently, customer-impacting network connectivity issues that occur within the MPLS core will be detected by the LSP Health Monitor.

Once configured, the LSP Health Monitor will automatically create and delete IP SLAs LSP ping or LSP traceroute operations based on network topology. The LSP Health Monitor feature also allows you to perform multioperation scheduling of IP SLAs operations and supports proactive threshold 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 113.

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

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

Prerequisites for the LSP Health Monitor

- The participating PE routers of an LSP Health Monitor operation must support the MPLS LSP ping feature. It is recommended that the Provider (P) routers also support the MPLS LSP Ping feature in order to obtain complete error reporting and diagnostics information. For more information about the MPLS LSP Ping feature, see the "Related Documents" section on page 35.
- Ensure that the source PE router has enough memory to support the desired LSP Health Monitor functionality. Enabling the LSP discovery option can potentially have a significant impact on router memory. If there is not enough memory available during the LSP discovery process, the process will gracefully terminate and an error message will be displayed.

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

Restrictions for the LSP Health Monitor

- The LSP Health Monitor with LSP Discovery feature supports Layer 3 MPLS VPNs only.
- The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE router. To prevent unnecessary router performance issues, careful consideration should be taken when configuring the operational and scheduling parameters of an LSP Health Monitor operation.
- Once an LSP Health Monitor operation is started, its configuration parameters should not be changed until the operation has ended. Changing the configuration parameters while the operation is actively running could cause delays in obtaining network connectivity statistics.
- The LSP discovery option does not support IP SLAs LSP traceroute operations.

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

- End-to-end LSP connectivity measurements across equal-cost multipaths for determining network availability or testing network connectivity in MPLS networks
- Proactive threshold monitoring through SNMP trap notifications and syslog messages
- Reduced network troubleshooting time for MPLS networks
- Scalable network error detection using fast retry capability
- Creation and deletion of IP SLAs operations based on network topology
- Discovery of Border Gateway Protocol (BGP) next hop neighbors based on local 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 configures an LSP Health Monitor operation and the BGP next hop neighbor discovery process is enabled.

   Configuring an LSP Health Monitor operation is similar to configuring a standard IP SLAs operation. To illustrate, all operation parameters for an LSP Health Monitor operation are configured after an identification number for the operation is specified. However, unlike standard IP SLAs operations, these configured parameters are then used as the base configuration for the individual IP SLAs LSP ping and LSP traceroute operations that will be created by the LSP Health Monitor. For more information on how to configure the LSP Health Monitor, see the "Configuring the LSP Health Monitor Without LSP Discovery" section on page 12 and "Configuring the LSP Health Monitor with LSP Discovery" section on page 17.

Note The LSP discovery process can potentially have a significant impact on the memory and CPU of the source PE router. To prevent unnecessary router performance issues, careful consideration should be taken when configuring the operational and scheduling parameters of an LSP Health Monitor operation.

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

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

2. The user configures proactive threshold monitoring parameters for the LSP Health Monitor operation. For more information about proactive threshold monitoring, see the "Proactive Threshold Monitoring for the LSP Health Monitor" section on page 9.

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

3. The user configures multioperation scheduling parameters for the LSP Health Monitor operation. For more information about multioperation scheduling, see the "Multioperation Scheduling for the LSP Health Monitor" section on page 11.

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

Addition and Deletion of IP SLAs Operations

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

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

Access Lists for Filtering BGP Next Hop Neighbors

Standard IP access lists can be configured (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 35.

Unique Identifier for Each Automatically Created IP SLAs Operation

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

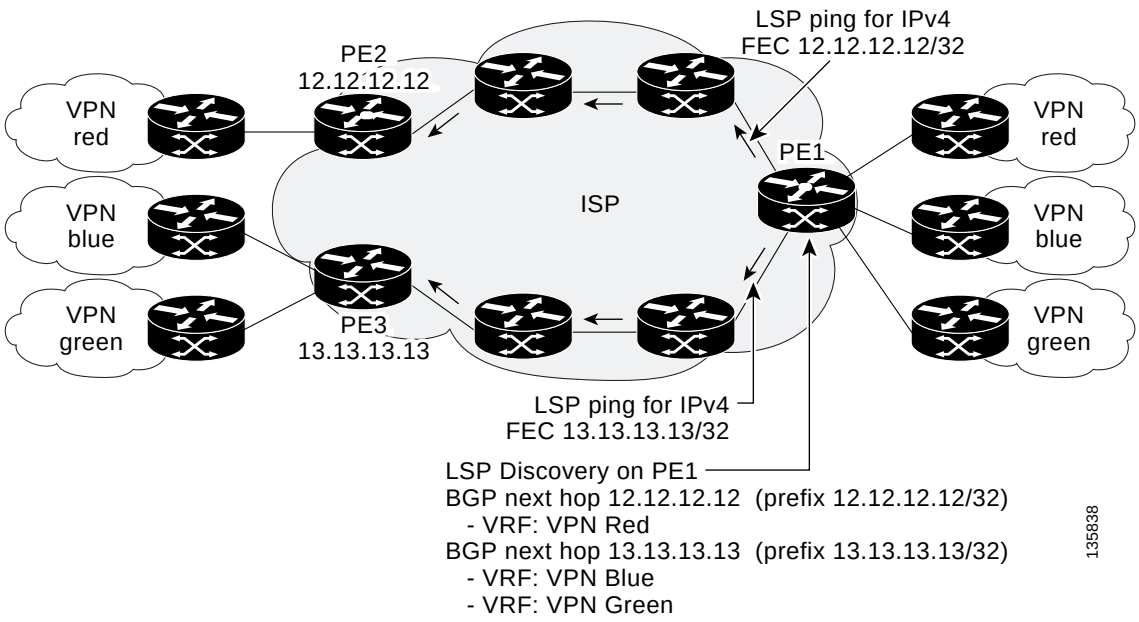
Discovery of Neighboring PE Routers

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

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

Figure 1 shows how the BGP next hop neighbor discovery process works for a simple VPN scenario for an Internet service provider (ISP). In this example, there are three VPNs associated with router PE1: red, blue, and green. From the perspective of router PE1, these VPNs are reachable remotely through BGP next hop neighbors PE2 (router ID: 12.12.12.12) and PE3 (router ID: 13.13.13.13). When the BGP next hop neighbor discovery process is enabled on router PE1, a database is generated based on the local VRF and global routing tables. The database in this example contains two BGP next hop router entries: PE2 12.12.12.12 and PE3 13.13.13.13. The routing entries are maintained per next hop router to distinguish 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 35.

Figure 1 BGP Next Hop Neighbor Discovery for a Simple VPN



The LSP Discovery Process

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

The general process for LSP discovery is as follows:

1. BGP next hop neighbors are discovered using the BGP next hop neighbor discovery process. For more information about the BGP next hop neighbor discovery process, see the "Discovery of Neighboring PE Routers" section on page 4.

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

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

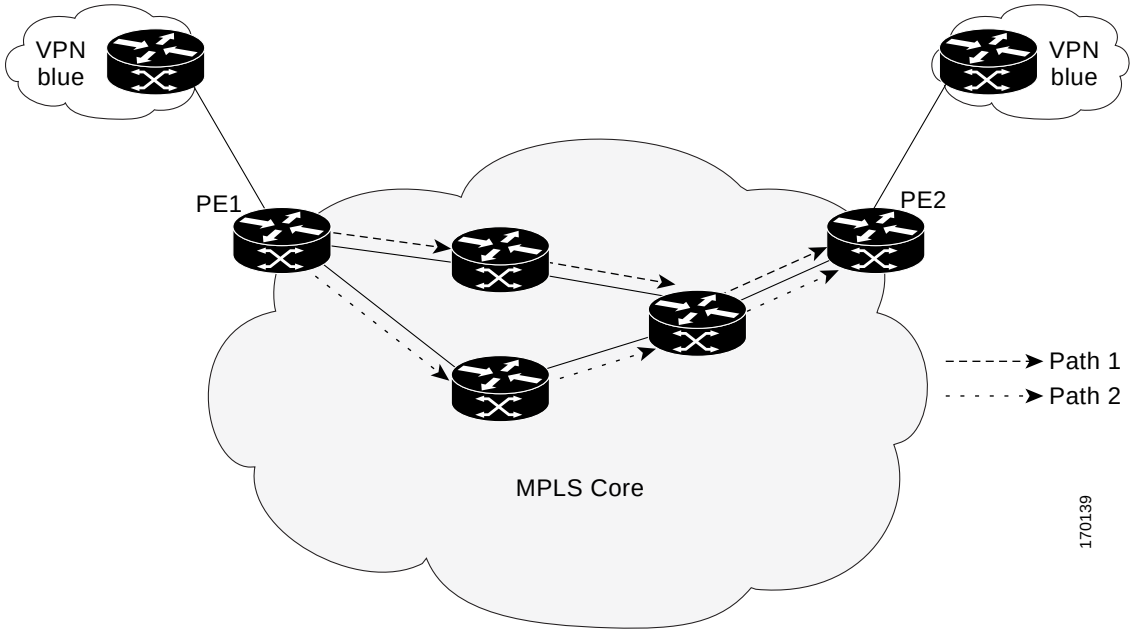
Note For a given LSP Health Monitor operation, the user can define the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery.

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

For information about proactive threshold monitoring and multioperation scheduling of IP SLAs operations created through the LSP discovery process, see the "Proactive Threshold Monitoring for the LSP Health Monitor" section on page 9 and "Multioperation Scheduling for the LSP Health Monitor" section on page 11.

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

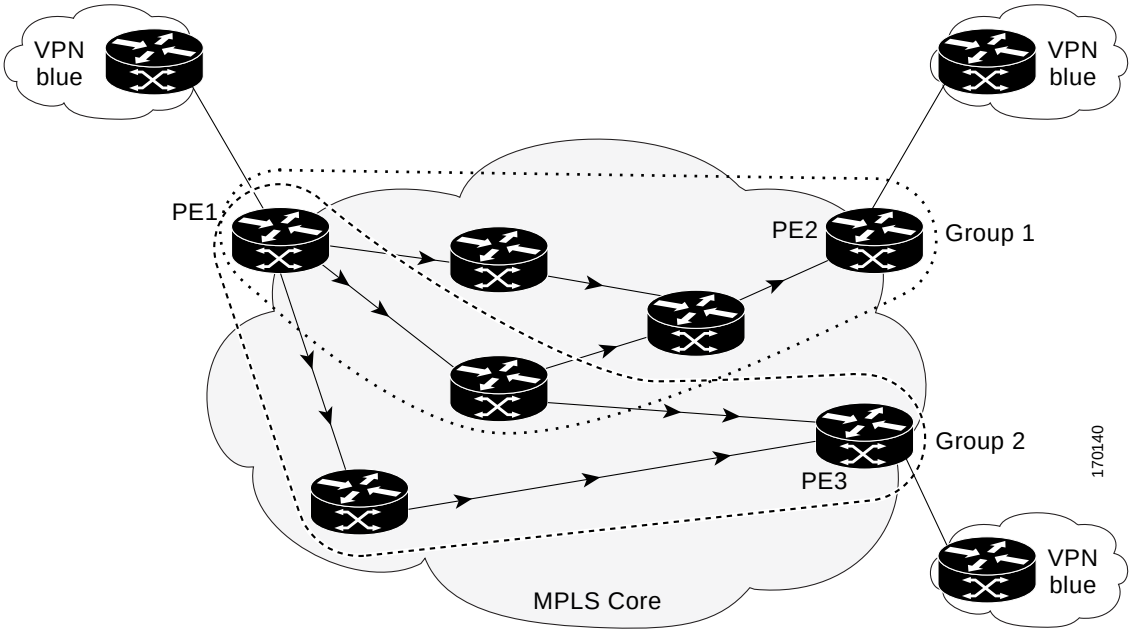
Figure 2 LSP Discovery for a Simple VPN



LSP Discovery Groups

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

Figure 3 LSP Discovery Groups for a Simple VPN



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

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

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

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

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

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

IP SLAs LSP Ping and LSP Traceroute Operations

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

For more information on how to configure IP SLAs operations using the LSP Health Monitor, see the "Configuring the LSP Health Monitor Without LSP Discovery" section on page 12 and the "Configuring the LSP Health Monitor with LSP Discovery" section on page 17. 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 21.

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 management tools, see the "Related Documents" section on page 35.

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

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 35.

LSP Discovery Option Enabled

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

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

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

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

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

Table 1 Conditions for Which an LSP Discovery Group Status Changes

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

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

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

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

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

Secondary Frequency Option

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

Multioperation Scheduling for the LSP Health Monitor

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

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 35.

LSP Discovery Option Enabled

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

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

The start times for the individual IP SLAs LSP ping operations for each LSP discovery group is based on the number of LSP discovery groups and the schedule period of the multioperation schedule. For example, if three LSP discovery groups (Group 1, Group 2, and Group 3) are scheduled to run over a period of 60 seconds, the first LSP ping operation of Group 1 will start at 0 seconds, the first LSP ping operation of Group 2 will start at 20 seconds, and the first LSP ping operation of Group 3 will start at 40 seconds. The remaining individual IP SLAs LSP ping operations for each LSP discovery group will run sequentially after completion of the first LSP ping operation. For each LSP discovery group, only one LSP ping operation runs at a time.

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

How to Use the LSP Health Monitor

This section contains the following tasks:

- Configuring the LSP Health Monitor Without LSP Discovery, page 12 (required)
- Configuring the LSP Health Monitor with LSP Discovery, page 17 (optional)

- Manually Configuring an IP SLAs LSP Ping or LSP Traceroute Operation, page 21 (optional)
- Verifying and Troubleshooting the LSP Health Monitor, page 25 (optional)

Configuring the LSP Health Monitor Without LSP Discovery

Perform this task to configure the operation parameters, reaction conditions, and scheduling options for an LSP Health Monitor operation without LSP discovery. If the LSP discovery option is disabled, only a single path between the source PE router and each BGP next hop neighbor is discovered. The LSP discovery option is disabled by default. 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** [**ipsla-vrf-all** | **vrf** *vpn-name*]
   or
   type pathEcho [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. **access-list** *access-list-number*
8. **scan-interval** *minutes*
9. **delete-scan-factor** *factor*
10. **force-explicit-null**
11. **exp** *exp-bits*
12. **lsp-selector** *ip-address*
13. **reply-dscp-bits** *dscp-value*
14. **reply-mode** {**ipv4** | **router-alert**}
15. **request-data-size** *bytes*
16. **secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency*
17. **tag** *text*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **ttl** *time-to-live*
21. **exit**
22. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}]

23. **auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh*:*mm*:*ss* | *hh*:*mm*[:*ss*] [*month day* | *day month*] | **now** | **pending**}]
24. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls discovery vpn next-hop** **Example:** `Router(config)# mpls discovery vpn next-hop`	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process. **Note** This command is automatically enabled when the **auto ip sla mpls-lsp-monitor** command is entered.
Step 4	**mpls discovery vpn interval** *seconds* **Example:** `Router(config)# mpls discovery vpn interval 120`	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN. The default time interval is 300 seconds.
Step 5	**auto ip sla mpls-lsp-monitor** *operation-number* **Example:** `Router(config)# auto ip sla mpls-lsp-monitor 1`	Begins configuration for an LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode. **Note** Entering this command automatically enables the **mpls discovery vpn next-hop** command.

Step 6	**type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*]
	or
	type pathEcho [**ipsla-vrf-all** | **vrf** *vpn-name*]
	
	Example:
	`Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`
	or
	
	Example:
	`Router(config-auto-ip-sla-mpls)# type pathEcho ipsla-vrf-all`
		Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.
		or
		Enters MPLS parameters configuration submode and allows the user to configure the parameters for an IP SLAs LSP traceroute operation using the LSP Health Monitor.

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

	Command or Action	Purpose
Step 9	**delete-scan-factor** *factor* **Example:** `Router(config-auto-ip-sla-mpls-params)# delete-scan-factor 2`	(Optional) Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid. The default scan factor is 1. In other words, each time the LSP Health Monitor checks the scan queue for updates, it deletes IP SLAs operations for BGP next hop neighbors that are no longer valid. If the scan factor is set to 0, IP SLAs operations will not be automatically deleted by the LSP Health Monitor. This configuration is not recommended. **Note** This command must be used with the **scan-interval** command.
Step 10	**force-explicit-null** **Example:** `Router(config-auto-ip-sla-mpls-params)# force-explicit-null`	(Optional) Adds an explicit null label to all echo request packets of an IP SLAs operation.
Step 11	**exp** *exp-bits* **Example:** `Router(config-auto-ip-sla-mpls-params)# exp 5`	(Optional) Specifies the experimental field value in the header for an echo request packet of an IP SLAs operation. The default experimental field value is 0.
Step 12	**lsp-selector** *ip-address* **Example:** `Router(config-auto-ip-sla-mpls-params)# lsp-selector 127.0.0.10`	(Optional) Specifies the local host IP address used to select the LSP of an IP SLAs operation. The default IP address is 127.0.0.0.
Step 13	**reply-dscp-bits** *dscp-value* **Example:** `Router(config-auto-ip-sla-mpls-params)# reply-dscp-bits 5`	(Optional) Specifies the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation. The default DSCP value is 0.
Step 14	**reply-mode** {**ipv4** | **router-alert**} **Example:** `Router(config-auto-ip-sla-mpls-params)# reply-mode router-alert`	(Optional) Specifies the reply mode for an echo request packet of an IP SLAs operation. The default reply mode is an IPv4 UDP packet.
Step 15	**request-data-size** *bytes* **Example:** `Router(config-auto-ip-sla-mpls-params)# request-data-size 200`	(Optional) Specifies the protocol data size for a request packet of an IP SLAs operation. For an IP SLAs LSP ping operation, the default is 100 bytes.

	Command or Action	Purpose
Step 16	**secondary-frequency** {**both** | **connection-loss** | **timeout**} *frequency* **Example:** `Router(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10`	(Optional) Sets the faster measurement frequency (secondary frequency) to which an IP SLAs operation should change when a reaction condition occurs.
Step 17	**tag** *text* **Example:** `Router(config-auto-ip-sla-mpls-params)# tag testgroup`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	**threshold** *milliseconds* **Example:** `Router(config-auto-ip-sla-mpls-params)# threshold 6000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 19	**timeout** *milliseconds* **Example:** `Router(config-auto-ip-sla-mpls-params)# timeout 7000`	(Optional) Specifies the amount of time the IP SLAs operation waits for a response from its request packet. The default timeout value is 5000 ms. **Note** The default timeout values vary by operation type.
Step 20	**ttl** *time-to-live* **Example:** `Router(config-auto-ip-sla-mpls-params)# ttl 200`	(Optional) Specifies the maximum hop count for an echo request packet of an IP SLAs operation.
Step 21	**exit** **Example:** `Router(config-auto-ip-sla-mpls-params)# exit`	Exits MPLS parameters configuration submode and returns to global configuration mode.
Step 22	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react** {**connectionLoss** | **timeout**} [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*] | **immediate** | **never**}] **Example:** `Router(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss action-type trapOnly threshold-type consecutive 3`	(Optional) Configures certain actions to occur based on events under the control of the LSP Health Monitor.

	Command or Action	Purpose
Step 23	**auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh*:*mm*:*ss* | *hh*:*mm*[:*ss*] [*month day* | *day month*] | **now** | **pending**}] **Example:** `Router(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now`	Configures the scheduling parameters for an LSP Health Monitor operation.
Step 24	**exit** **Example:** `Router(config)# exit`	Exits global configuration submode and returns to privileged EXEC mode.

Troubleshooting Tips

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

What to Do Next

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

Configuring the LSP Health Monitor with LSP Discovery

Perform this task to configure the operation parameters, reaction conditions, and scheduling options for an LSP Health Monitor operation with LSP discovery. If the LSP discovery option is enabled, the equal-cost multipaths between the source PE router and each BGP next hop neighbor are discovered. If the LSP discovery option is disabled, only a single path between the source PE router and each BGP next hop neighbor is discovered. The LSP discovery option is disabled by default. 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** [**ipsla-vrf-all** | **vrf** *vpn-name*]
7. Configure optional parameters for the IP SLAs LSP echo operation. See Steps 7 through 21 in the "Configuring the LSP Health Monitor Without LSP Discovery" section on page 12.
8. **path-discover**
9. **hours-of-statistics-kept** *hours*
10. **force-explicit-null**
11. **interval** *milliseconds*
12. **lsp-selector-base** *ip-address*
13. **maximum-sessions** *number*
14. **scan-period** *minutes*
15. **session-timeout** *seconds*
16. **timeout** *seconds*
17. **exit**
18. **exit**
19. **auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**]
20. **ip sla logging traps**
21. **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**}]
22. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls discovery vpn next-hop** **Example:** `Router(config)# mpls discovery vpn next-hop`	(Optional) Enables the MPLS VPN BGP next hop neighbor discovery process. **Note** This command is automatically enabled when the **auto ip sla mpls-lsp-monitor** command is entered.
Step 4	**mpls discovery vpn interval** *seconds* **Example:** `Router(config)# mpls discovery vpn interval 120`	(Optional) Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN. The default time interval is 300 seconds.
Step 5	**auto ip sla mpls-lsp-monitor** *operation-number* **Example:** `Router(config)# auto ip sla mpls-lsp-monitor 1`	Begins configuration for an LSP Health Monitor operation and enters auto IP SLAs MPLS configuration mode. **Note** Entering this command automatically enables the **mpls discovery vpn next-hop** command.
Step 6	**type echo** [**ipsla-vrf-all** | **vrf** *vpn-name*] **Example:** `Router(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all`	Enters MPLS parameters configuration mode and allows the user to configure the parameters for an IP SLAs LSP ping operation using the LSP Health Monitor.
Step 7	Configure optional parameters for the IP SLAs LSP echo operation. See Steps 7 through 21 in the "Configuring the LSP Health Monitor Without LSP Discovery" section on page 12.	(Optional) Configures optional parameters for an IP SLAs LSP echo operation.
Step 8	**path-discover** **Example:** `Router(config-auto-ip-sla-mpls-params)# path-discover`	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters LSP discovery parameters configuration submode.
Step 9	**hours-of-statistics-kept** *hours* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# hours-of-statistics-kept 1`	(Optional) Sets the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.
Step 10	**force-explicit-null** **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# force-explicit-null`	(Optional) Adds an explicit null label to all echo request packets of an LSP Health Monitor operation.

	Command or Action	Purpose
Step 11	**interval** *milliseconds* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# interval 2`	(Optional) Specifies the time interval between MPLS echo requests that are sent as part of the LSP discovery process for an LSP Health Monitor operation.
Step 12	**lsp-selector-base** *ip-address* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# lsp-selector-base 127.0.0.2`	(Optional) Specifies the base IP address used to select the LSPs belonging to the LSP discovery groups of an LSP Health Monitor operation.
Step 13	**maximum-sessions** *number* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# maximum-sessions 2`	(Optional) Specifies the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation. **Note** Careful consideration should be used when configuring this parameter to avoid a negative impact on the router's CPU.
Step 14	**scan-period** *minutes* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# scan-period 30`	(Optional) Sets the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.
Step 15	**session-timeout** *seconds* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# session-timeout 60`	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its LSP discovery request for a particular BGP next hop neighbor.
Step 16	**timeout** *seconds* **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# timeout 4`	(Optional) Sets the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its echo request packets. **Note** Careful consideration should be used when configuring this parameter to avoid a negative impact on the router's CPU.
Step 17	**exit** **Example:** `Router(config-auto-ip-sla-mpls-lpd-params)# exit`	Exits LSP discovery parameters configuration submode and returns to MPLS parameters configuration mode.
Step 18	**exit** **Example:** `Router(config-auto-ip-sla-mpls-params)# exit`	Exits MPLS parameters configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 19	**auto ip sla mpls-lsp-monitor reaction-configuration** *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**] **Example:** `Router(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type trapOnly`	(Optional) Configures the proactive threshold monitoring parameters for an LSP Health Monitor operation with LSP discovery enabled.
Step 20	**ip sla logging traps** **Example:** `Router(config)# ip sla logging traps`	(Optional) Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
Step 21	**auto ip sla mpls-lsp-monitor schedule** *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh*:*mm*:*ss* | *hh*:*mm*[:*ss*] [*month day* | *day month*] | **now** | **pending**}] **Example:** `Router(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now`	Configures the scheduling parameters for an LSP Health Monitor operation.
Step 22	**exit** **Example:** `Router(config)# exit`	Exits global configuration submode and returns to privileged EXEC mode.

Troubleshooting Tips

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

What to Do Next

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

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

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** *operation-number* **Example:** `Router(config)# ip sla 1`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

Step 4	**mpls lsp ping ipv4** *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
	or
	mpls lsp trace ipv4 *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]
	
	Example:
	`Router(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
	or
	
	Example:
	`Router(config-ip-sla)# mpls lsp trace ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1`
		Configures the IP SLAs operation as an LSP ping operation and enters LSP ping configuration mode.
		or
		Configures the IP SLAs operation as an LSP trace operation and enters LSP trace configuration mode.

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

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

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

Troubleshooting Tips

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

What to Do Next

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

Verifying and Troubleshooting the LSP Health Monitor

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**debug ip sla error** [*operation-number*] **Example:** `Router# debug ip sla error`	(Optional) Enables debugging output of IP SLAs operation run-time errors.
Step 2	**debug ip sla mpls-lsp-monitor** [*operation-number*] **Example:** `Router# debug ip sla mpls-lsp-monitor`	(Optional) Enables debugging output of LSP Health Monitor operations.
Step 3	**debug ip sla trace** [*operation-number*] **Example:** `Router# debug ip sla trace`	(Optional) Enables debugging output for tracing the execution of IP SLAs operations.
Step 4	**show ip sla mpls-lsp-monitor collection-statistics** [*group-id*] **Example:** `Router# show ip sla mpls-lsp-monitor collection-statistics 100001`	(Optional) Displays the statistics for IP SLAs operations belonging to an LSP discovery group of an LSP Health Monitor operation. **Note** This command is applicable only if the LSP discovery option is enabled.
Step 5	**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 6	**show ip sla mpls-lsp-monitor lpd operational-state** [*group-id*] **Example:** `Router# show ip sla mpls-lsp-monitor lpd operational-state 100001`	(Optional) Displays the operational status of the LSP discovery groups belonging to an LSP Health Monitor operation. **Note** This command is applicable only if the LSP discovery option is enabled.
Step 7	**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 8	**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.

	Command or Action	Purpose
Step 9	**show ip sla mpls-lsp-monitor summary** [*operation-number* [**group** [*group-id*]]] **Example:** `Router# show ip sla mpls-lsp-monitor summary`	(Optional) Displays BGP next hop neighbor and LSP discovery group information for LSP Health Monitor operations. **Note** This command is applicable only if the LSP discovery option is enabled.
Step 10	**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. **Note** This command applies only to manually configured IP SLAs operations.
Step 11	**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. **Note** This command applies only to manually configured IP SLAs operations.
Step 12	**show mpls discovery vpn** **Example:** `Router# show mpls discovery vpn`	(Optional) Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

Configuration Examples for the LSP Health Monitor

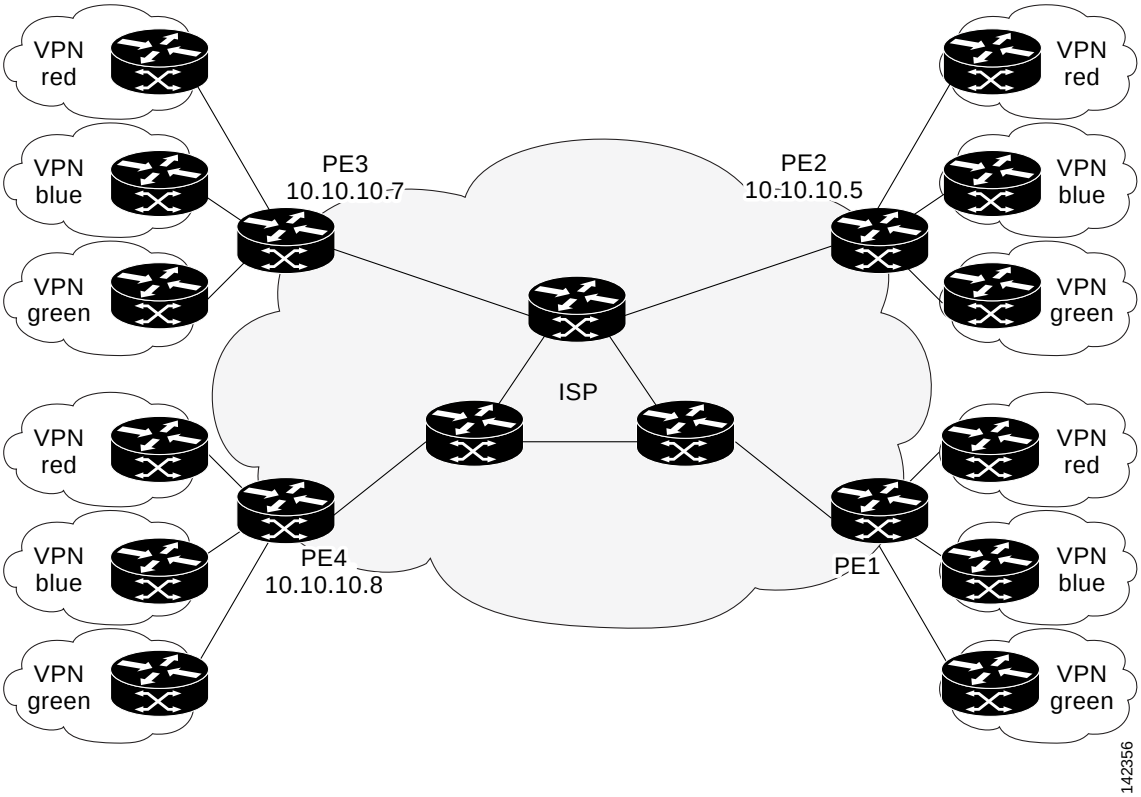
This section provides the following configuration examples:

- Configuring and Verifying the LSP Health Monitor Without LSP Discovery: Example, page 27
- Configuring and Verifying the LSP Health Monitor with LSP Discovery: Example, page 31
- Manually Configuring an IP SLAs LSP Ping Operation: Example, page 34

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

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

Figure 4 Network Used for LSP Health Monitor Example



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

Router PE1 Configuration

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

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

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

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

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

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

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

```
PE1# show mpls discovery vpn

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

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

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

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

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
```

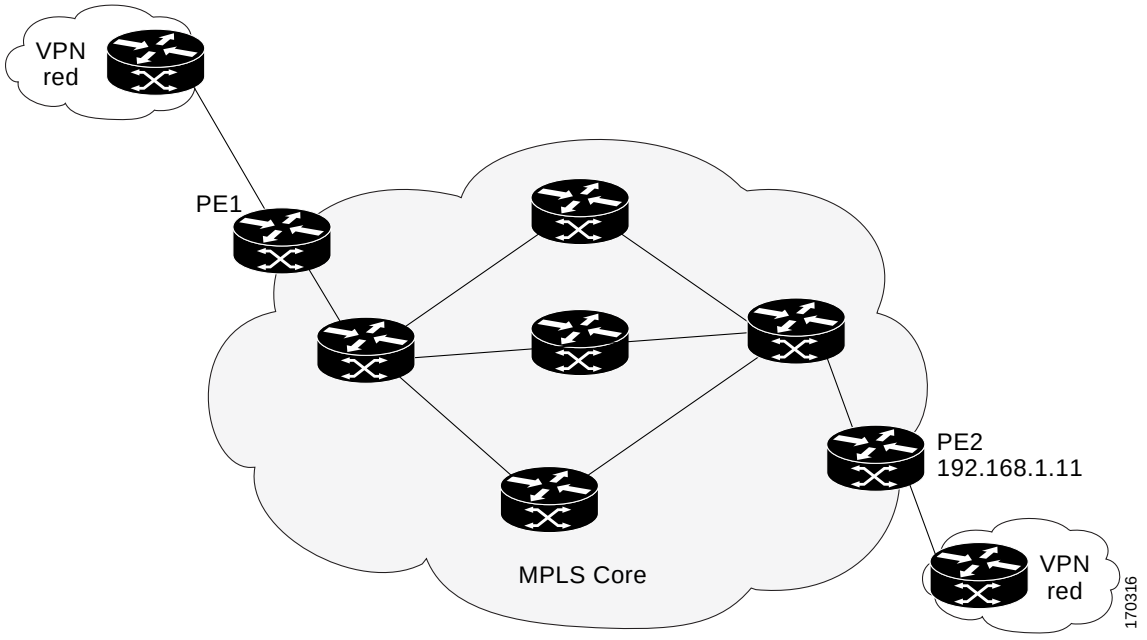
```
PE1# debug ip sla mpls-lsp-monitor

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
```

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

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

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



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

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

Router PE1 Configuration

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

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

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

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

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

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

```
PE1# show mpls discovery vpn

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

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

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

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

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

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

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

Entry number: 100001
MPLSLM Entry Number: 100
Target FEC Type: LDP IPv4 prefix
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :
Path   Outgoing   Lsp             Link  Conn  Adj             Downstream
Index  Interface  Selector        Type  Id    Addr            Label Stack     Status
1      Et0/0      127.0.0.8       90    0     10.10.18.30     21              OK
2      Et0/0      127.0.0.2       90    0     10.10.18.30     21              OK
3      Et0/0      127.0.0.1       90    0     10.10.18.30     21              OK
```

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

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

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

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

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

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

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

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

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

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

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

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

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 with LSP Discovery feature.

Related Documents

Related Topic	Document Title
MPLS LSP ping and LSP traceroute management tools	*MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV*, Cisco IOS feature module, Release 12.2(33)SRB
MPLS LSP discovery management tool	*MPLS EM—MPLS LSP Multipath Tree Trace*, Cisco IOS feature module, Release 12.2(33)SRB
Configuring standard IP access lists	"IP Access Lists" chapter of the *Cisco IOS IP Application Services Configuration Guide*, Release 12.4
Multioperation scheduling for Cisco IOS IP SLAs	"IP SLAs—Multioperation Scheduling of IP SLAs Operations" chapter of the *IP SLAs Configuration Guide*, Release 12.4T
Proactive threshold monitoring for Cisco IOS IP SLAs	"IP SLAs—Proactive Threshold Monitoring of IP SLAs Operations" chapter of the *IP SLAs Configuration Guide*, Release 12.4T
Cisco IOS IP SLAs command line interface enhancements	*Cisco IOS IP Service Level Agreements Command Line Interface*, Cisco white paper
Cisco IOS IP SLAs configuration tasks	*Cisco IOS IP SLAs Configuration Guide*, Release 12.4T
Cisco IOS IP SLAs commands	*Cisco IOS IP SLAs Command Reference*, Release 12.2SR

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **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**
- **hours-of-statistics-kept (LSP discovery)**
- **interval (LSP discovery)**
- **lsp-selector**
- **lsp-selector-base**
- **maximum-sessions**
- **mpls discovery vpn interval**
- **mpls discovery vpn next-hop**
- **mpls lsp ping ipv4**
- **mpls lsp trace ipv4**

- path-discover
- reply-dscp-bits
- reply-mode
- scan-interval
- scan-period
- secondary-frequency
- session-timeout (LSP discovery)
- show ip sla mpls-lsp-monitor collection-statistics
- show ip sla mpls-lsp-monitor configuration
- show ip sla mpls-lsp-monitor lpd operational-state
- show ip sla mpls-lsp-monitor neighbors
- show ip sla mpls-lsp-monitor scan-queue
- show ip sla mpls-lsp-monitor summary
- show mpls discovery vpn
- timeout (LSP discovery)
- 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 auto IP SLA MPLS parameters 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

access-list-number	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 parameters configuration (config-auto-ip-sla-mpls-params)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 VPN routing or forwarding instances (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.

```
!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
```

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.

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 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

operation-number	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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr mpls-lsp-monitor** command.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr mpls-lsp-monitor** command.

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, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (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 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 proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **auto ip sla mpls-lsp-monitor reaction-configuration** command in global configuration mode. To clear all threshold monitoring configuration for a specified LSP Health Monitor operation, use the **no** form of this command.

LSP Health Monitor Without LSP Discovery

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

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

LSP Health Monitor with LSP Discovery

auto ip sla mpls-lsp-monitor reaction-configuration *operation-number* **react lpd** {**lpd-group** [**retry** *number*] | **tree-trace**} [**action-type trapOnly**]

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

Syntax Description

operation-number	Number of the LSP Health Monitor operation for which reactions are to be configured.
react connectionLoss	Enables monitoring of one-way connection loss events.
react timeout	Enables monitoring of one-way timeout events.
action-type *option*	(Optional) Specifies what action is performed when threshold events occur. If the **threshold-type never** keywords are defined, the **action-type** keyword is disabled. The *option* argument can be one of the following keywords: • **none**—No action is taken. This option is the default value. • **trapOnly**—SNMP trap notification is sent.
threshold-type consecutive [*occurrences*]	(Optional) When a threshold violation for the monitored element (such as a timeout) 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 *occurrences* argument. The valid range is from 1 to 16.
threshold-type immediate	(Optional) When a threshold violation for the monitored element (such as a timeout) 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.
lpd	(Optional) Specifies the LSP discovery option.
lpd-group	(Optional) Enables monitoring of LSP discovery group status changes.

retry *number*	(Optional) Specifies the number of times the equal-cost multipaths belonging to an LSP discovery group are retested when a failure is detected. After the specified number of retests have been completed, an SNMP trap notification may be sent depending on the current status of the LSP discovery group. See the "Usage Guidelines" section for more information. The value of the *number* argument is zero by default. Use the **secondary frequency** command to increase the frequency at which failed paths belonging to an LSP discovery group are retested. This command is not applicable if the retry value is set to zero.
tree-trace	(Optional) Enables monitoring of situations where LSP discovery to a Border Gateway Protocol (BGP) next hop neighbor fails.
action-type trapOnly	(Optional) Enables SNMP trap notifications.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr mpls-lsp-monitor reaction-configuration** command.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr mpls-lsp-monitor reaction-configuration** command.

Usage Guidelines

You can configure the **auto ip sla mpls-lsp-monitor reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements for the same operation. However, disabling of individual monitored elements is not supported. In other words, the **no auto ip sla mpls-lsp-monitor reaction-configuration** command will disable all proactive threshold monitoring configuration for the specified IP SLAs operation.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Depending on the Cisco IOS software release that you are running, use the **ip sla logging traps** or **ip sla monitor logging traps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-server enable traps rtr** command to enable the sending of IP SLAs SNMP trap notifications.

To display the current threshold monitoring configuration settings for an LSP Health Monitor operation, use the **show ip sla mpls-lsp-monitor configuration** command.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss or timeout events occur, an SNMP trap notification 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.
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
ip sla monitor logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.
snmp-server enable traps rtr	Enables the sending of IP SLAs SNMP trap notifications.

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 [**lpd** *group-number*]

Syntax Description

lpd *group-number*	(Optional) Specifies the number used to identify the LSP discovery group you wish to configure.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **lpd** keyword and *lpd-group* argument was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **auto ip sla mpls-lsp-monitor reset lpd** *group-number* command to remove all the stored network connectivity statistics for the specified LSP discovery group from the LSP discovery group database. The non-statistical LSP discovery group data will be set to default values or zero. However, the IP address of the associated Border Gateway Protocol (BGP) next hop neighbor, the list of LSP discovery group IP SLAs operations, and the list of LSP selector IP addresses will be preserved. After the **auto ip sla mpls-lsp-monitor reset lpd** *group-number* command is entered, statistical data for the group will start aggregating again with new data only.

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

operation-number	Number of the LSP Health Monitor operation to be scheduled.
schedule-period *seconds*	Specifies the amount of time (in seconds) for which the LSP Health Monitor is scheduled.
frequency *seconds*	(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 *hh*:*mm*:*ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
hh:*mm*[:*ss*]	(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.
month	(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.
day	(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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr mpls-lsp-monitor schedule** command.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr mpls-lsp-monitor schedule** command.

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, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The schedule period for LSP Health Monitor operation 1 is set to 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

operation-number	(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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **debug rtr mpls-lsp-monitor** command.

Examples

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

```
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 auto IP SLA MPLS parameters 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

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.

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

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

This command must be used with the **scan-interval** command. Use the **scan-interval** command 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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (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.

```
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
```

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.
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.

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 or IP SLA configuration mode. To return to the default value, use the **no** form of this command.

exp *exp-bits*

no exp

Syntax Description

exp-bits	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 and IP SLA Monitor Configuration

LSP ping configuration (config-sla-monitor-lspPing)
LSP trace configuration (config-sla-monitor-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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 2). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see Table 3 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 2 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, 12.0(32)SY, 12.2(33)SRB, or later releases	**ip sla**	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, or 12.2(31)SB2	**ip sla monitor**	IP SLA monitor configuration

Table 3 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, 12.0(32)SY, 12.2(31)SB2, 12.2(33)SRB, or later releases	**auto ip sla mpls-lsp-monitor**	Auto IP SLA MPLS configuration

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (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.

```
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
```

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.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor 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 appropriate submode of auto IP SLA 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)
LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. Support for this command in MPLS label switched path (LSP) discovery parameters configuration mode was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source PE router. In this example, an explicit null label will be added to all the echo request packets of IP SLAs operations created by LSP Health Monitor operation 1.

```
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
```

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.

hours-of-statistics-kept (LSP discovery)

To set the number of hours for which label switched path (LSP) discovery group statistics are maintained for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **hours-of-statistics-kept** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

hours-of-statistics-kept *hours*

no hours-of-statistics-kept

Syntax Description

hours	Number of hours that statistics are maintained. The default is 2 hours.

Command Default

2 hours

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The LSP discovery group statistics are distributed in one-hour increments. Since the number of LSP discovery groups for a single LSP Health Monitor operation can be significantly large, the collection of group statistics is restricted to a maximum of 2 hours. If the *number* argument is set to zero, no LSP discovery group statistics are maintained.

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. LSP discovery group statistics are collected every 1 hour.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
```

```
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

interval (LSP discovery)

To specify the time interval between Multiprotocol Label Switching (MPLS) echo requests that are sent as part of the label switched path (LSP) discovery process for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **interval** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

interval *milliseconds*

no interval

Syntax Description

milliseconds	Number of milliseconds between each MPLS echo request. The default is 0 milliseconds.

Command Default

0 milliseconds

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. To discover the equal cost multipaths per BGP next hop neighbor, MPLS echo requests are sent every 2 milliseconds.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
```

```
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters 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 auto IP SLA MPLS parameters 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

ip-address	Specifies a local host IP address used to select the LSP.

Command Default

The local host IP address used to select the LSP is 127.0.0.0.

Command Modes

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

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 equal-cost multipaths between the source Provider Edge (PE) router and the Border Gateway Protocol (BGP) next hop neighbor.

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (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.

```
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 127.0.0.1
!
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.

lsp-selector-base

To specify the base IP address used to select the label switched paths (LSPs) belonging to the LSP discovery groups of a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **lsp-selector-base** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

lsp-selector-base *ip-address*

no lsp-selector-base

Syntax Description

ip-address	Base IP address used to select the LSPs within an LSP discovery group. The default IP address is 127.0.0.0.

Command Default

The default base IP address is 127.0.0.0.

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Each equal-cost multipath belonging to an LSP discovery group is uniquely identified by the following three parameters:

- Local host IP address of the LSP selector
- Outgoing interface
- Downstream MPLS label stack number

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The base IP address used to select the LSPs within the LSP discovery groups is set to 127.0.0.2.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
```

```
 maximum-sessions 2
 session-timeout 60
 lsp-selector-base 127.0.0.2
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now

auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

maximum-sessions

To specify the maximum number of Border Gateway Protocol (BGP) next hop neighbors that can be concurrently undergoing label switched path (LSP) discovery for a single Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **maximum-sessions** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

maximum-sessions *number*

no maximum-sessions

Syntax Description

number	Maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery. The default is 1.

Command Default

By default, the *number* argument is set to 1.

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The maximum number of LSP discovery processes allowed to run concurrently is set to 2.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
```

```
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters 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

seconds	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. The default is 300 seconds.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 VPN routing or forwarding instance (VRF) associated with the source Provider Edge (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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

When the BGP next hop neighbor discovery process is enabled, a database of BGP next hop neighbors in use by any VPN routing or forwarding instance (VRF) associated with the source Provider Edge (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

destination-address	Address prefix of the target to be tested.
destination-mask	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 *ip-address*	(Optional) Specifies a local host IP address used to select the LSP. Default address is 127.0.0.1
src-ip-addr *source-address*	(Optional) Specifies a source IP address for the echo request originator.
reply dscp *dscp-value*	(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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type mpls lsp ping ipv4** command.

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

destination-address	Address prefix of the target to be tested.
destination-mask	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 *ip-address*	(Optional) Specifies a local host IP address used to select the LSP. Default address is 127.0.0.1.
src-ip-addr *source-address*	(Optional) Specifies a source IP address for the echo request originator.
reply dscp *dscp-value*	(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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **mpls lsp trace ipv4** command.

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.

path-discover

To enable the label switched path (LSP) discovery option for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode, use the **path-discover** command in auto IP SLA MPLS parameters configuration mode. To disable the LSP discovery option, use the **no** form of this command.

path-discover

no path-discover

Syntax Description

This command has no arguments or keywords.

Command Default

The LSP discovery option is disabled.

Command Modes

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

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to enable the LSP discovery option of IP SLAs LSP Health Monitor operation 1:

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
```

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.

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 auto IP SLA MPLS parameters 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

dscp-value	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 parameters configuration (config-auto-ip-sla-mpls-params)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (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.

```
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
```

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.

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

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. 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.

```
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
```

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.

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 Border Gateway Protocol (BGP) next hop neighbor updates, use the **scan-interval** command in auto IP SLA MPLS parameters configuration mode. To return to the default value, use the **no** form of this command.

scan-interval *minutes*

no scan-interval

Syntax Description

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

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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.

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute.

```
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
```

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.
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.

scan-period

To set the amount of time after which the label switched path (LSP) discovery process can restart for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **scan-period** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

scan-period *minutes*

no scan-period

Syntax Description

minutes	The amount of time (in minutes) after which the LSP discovery process can restart. The default is 1 minute.

Command Default

1 minute

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

When the LSP discovery process has completed one iteration of discovering the equal-cost multipaths for each applicable Border Gateway Protocol (BGP) next hop neighbors associated with a single LSP Health Monitor operation, the next iteration of the LSP discovery process will start immediately if the time period set by the **scan-period** command has expired. If this rediscovery time period has not yet expired, then the next iteration of the LSP discovery process will not start until the time period has expired.

Setting the LSP rediscovery time period to 0 will cause the LSP discovery process to always restart immediately after completing one iteration of discovering the equal-cost multipaths for each applicable BGP next hop neighbor associated with a single LSP Health Monitor operation.

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The LSP rediscovery time period is set to 30 minutes.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
```

```
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

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 or IP SLA 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.
frequency	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 and IP SLA Monitor Configuration

LSP ping configuration (config-sla-monitor-lspPing)
LSP trace configuration (config-sla-monitor-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. The **both** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 path, the frequency at which the path is remeasured will increase to the secondary frequency value (testing at a faster rate). When the configured reaction condition is met (such as N consecutive connection losses or N consecutive timeouts), an SNMP trap and syslog message can be sent and the measurement frequency will return to its original frequency value.

Note By default, 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.

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 4). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see Table 5 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 4 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, 12.0(32)SY, 12.2(33)SRB, or later releases	**ip sla**	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, or 12.2(31)SB2	**ip sla monitor**	IP SLA monitor configuration

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, 12.0(32)SY, 12.2(31)SB2, 12.2(33)SRB, or later releases	**auto ip sla mpls-lsp-monitor**	Auto IP SLA MPLS configuration

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (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.

```
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
```

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

session-timeout (LSP discovery)

To set the amount of time the label switched path (LSP) discovery process for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation waits for a response to its LSP discovery request for a particular Border Gateway Protocol (BGP) next hop neighbor, use the **session-timeout** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

session-timeout *seconds*

no session-timeout

Syntax Description

seconds	The amount of time (in seconds) an LSP Health Monitor operation waits for a response to its LSP discovery request. The default value is 120 seconds.

Command Default

120 seconds

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Before an LSP discovery group is created for a particular BGP next hop neighbor, the LSP Health Monitor must receive a response to its LSP discovery request for that BGP next hop neighbor. If no response is received within the specified time limit, the LSP discovery process is not performed for that particular BGP next hop neighbor.

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The timeout value for the LSP discovery requests is set to 60 seconds.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
```

```
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

show ip sla mpls-lsp-monitor collection-statistics

To display the statistics for Cisco IOS IP Service Level Agreements (SLAs) operations belonging to a label switched path (LSP) discovery group of an LSP Health Monitor operation, use the **show ip sla mpls-lsp-monitor collection-statistics** command in user EXEC or privileged EXEC mode.

show ip sla mpls-lsp-monitor collection-statistics [*group-id*]

Syntax Description

group-id	(Optional) Identification number of the LSP discovery group for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Use the **show ip sla mpls-lsp-monitor collection-statistics** command if the LSP discovery option is enabled for an LSP Health Monitor operation. This command is not applicable if the LSP discovery option is disabled.

When the LSP discovery option is enabled, an individual IP SLAs operation is created by the LSP Health Monitor for each equal-cost multipath belonging to an LSP discovery group of a particular LSP Health Monitor operation. The network connectivity statistics collected by each individual IP SLAs operation are aggregated and stored in one-hour increments (data can be collected for a maximum of two hours). Results are stored as group averages representative of all the equal-cost multipaths within the group for a given one-hour increment.

Examples

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

```
Router# show ip sla mpls-lsp-monitor collection-statistics 100001

Entry number: 100001
Start Time Index: *19:32:37.995 EST Mon Feb 28 2005
Path Discovery Start Time: *20:23:43.919 EST Mon Feb 28 2005
Target destination IP address: 10.131.161.251
Path Discovery Status: OK
Path Discovery Completion Time: 1772
Path Discovery Minimum Paths: 12
Path Discovery Maximum Paths: 12
LSP Group Index: 100001
LSP Group Status: up
Total Pass: 1225
Total Timeout: 0 Total Fail: 0
Latest probe status: 'up,up,up,up,up,up,up,up,up,up,up,up'
```

```
Latest Path Identifier:
'127.0.0.13-Se3/0-38,127.0.0.6-Se3/0-38,127.0.0.1-Se3/0-38,127.0.0.2-Se3/0-38,127.0.0.4-Se
3/0-38,127.0.0.5-Se3/0-38,127.0.0.13-Se4/0-38,127.0.0.6-Se4/0-38,127.0.0.1-Se4/0-38,127.0.
0.2-Se4/0-38,127.0.0.4-Se4/0-38,127.0.0.5-Se4/0-38'
Minimum RTT: 24 Maximum RTT: 100 Average RTT: 42
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip sla mpls-lsp-monitor collection-statistics Field Descriptions

Field	Description
Entry number	Identification number of the LSP discovery group.
Start Time Index	Start time of the LSP Health Monitor operation.
Path Discovery Start Time	Time in which the most recent iteration of LSP discovery started.
Target destination IP address	IP address of the Border Gateway Protocol (BGP) next hop neighbor.
Path Discovery Status	Return code of the most recent iteration of LSP discovery.
Path Discovery Completion Time	Amount of time (in milliseconds) it took to complete the most recent iteration of the LSP discovery process.
Path Discovery Minimum Paths	Minimum number of equal-cost multipaths discovered by the LSP discovery process.
Path Discovery Maximum Paths	Maximum number of equal-cost multipaths discovered by the LSP discovery process.
LSP Group Index	Identification number of the LSP discovery group.
LSP Group Status	Operation status of the LSP discovery group.
Total Pass	Total number of LSP discovery process iterations.
Total Timeout	Total number of LSPs in which a timeout violation was reported.
Total Fail	Total number of LSPs in which an operation failure was reported.
Latest probe status	Current operation status for each IP SLAs operation belonging to the specified LSP discovery group.
Latest Path Identifier	Current identification information (IP address used to select the LSP, outgoing interface, and label stack) for each IP SLAs operation belonging to the specified LSP discovery group.
Minimum RTT	Minimum round-trip time (in milliseconds) measured by the IP SLAs operations associated with the specified LSP discovery group.
Maximum RTT	Maximum round-trip time (in milliseconds) measured by the IP SLAs operations associated with the specified LSP discovery group.
Average RTT	Average round-trip time (in milliseconds) for all the IP SLAs operations associated with the specified LSP discovery group.

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

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

operation-number	(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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr mpls-lsp-monitor configuration** command.

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 7 describes the significant fields shown in the display.

Table 7 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 ipsla-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 an IP SLAs 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)	Upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
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 of the IP SLAs operations created by the LSP Health Monitor operation.
Schedule Period(sec)	Time period (in seconds) in which the start times of the individual IP SLAs operations are distributed.

Table 7 show ip sla mpls-lsp-monitor configuration Field Descriptions (continued)

Field	Description
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.
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 lpd operational-state

To display the operational status of the label switched path (LSP) discovery groups belonging to an IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **show ip sla mpls-lsp-monitor lpd operational-state** command in user EXEC or privileged EXEC mode.

show ip sla mpls-lsp-monitor lpd operational-state [*group-id*]

Syntax Description

group-id	(Optional) Identification number of the LSP discovery group for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Use the **show ip sla mpls-lsp-monitor lpd operational-state** command if the LSP discovery option is enabled for an LSP Health Monitor operation. This command is not applicable if the LSP discovery option is disabled.

Examples

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

```
Router# show ip sla mpls-lsp-monitor lpd operational-state 100001

Entry number: 100001
MPLSLM Entry Number: 1
Target FEC Type: LDP IPv4 prefix
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :
Path   Outgoing   Lsp       Link  Conn  Adj   Downstream
Index  Interface  Selector  Type  Id    Addr  Label Stack  Status
1 Et0/0 127.0.0.8 90 0 10.10.18.30 21 OK
2 Et0/0 127.0.0.2 90 0 10.10.18.30 21 OK
3 Et0/0 127.0.0.1 90 0 10.10.18.30 21 OK
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip sla mpls-lsp-monitor lpd operational-state Field Descriptions

Field	Description
Entry number	Identification number of the LSP discovery group.
MPLSLM Entry number	Identification number of the LSP Health Monitor operation.
Target FEC Type	The Forward Equivalence Class (FEC) type of the BGP next hop neighbor.
Target Address	IP address of the Border Gateway Protocol (BGP) next hop neighbor.
Number of Statistic Hours Kept	The amount of time (in hours) in which LSP discovery group statistics will be maintained. Use the **hours-of-statistics-kept** command to configure this value.
Traps Type	Trap type values indicate the type of threshold monitoring that has been enabled using the **auto ip sla mpls-lsp-monitor reaction-configuration** command. Trap type values are defined as follows: • 1—timeout • 2—connection loss • 3—LSP discovery group status changes • 4—LSP discovery failure
Latest Path Discovery Mode	Current mode of the LSP discovery process. Modes include initial discovery, initial complete, rediscovery running, and rediscovery complete.
Latest Path Discovery Start Time	Time in which the most recent iteration of LSP discovery started.
Latest Path Discovery Return Code	Return code for the most recent iteration of LSP discovery.
Latest Path Discovery Completion Time	Amount of time (in milliseconds) it took to complete the most recent iteration of the LSP discovery process.
Number of Paths Discovered	Number of equal-cost multipaths discovered during the most recent iteration of the LSP discovery process.
Path Index	Identification number for the equal-cost multipath.
Outgoing Interface	Outgoing interface of the echo request packet.
Lsp Selector	IP address used to select the LSP.
Adj Addr	IP address of the next hop physical interface.
Downstream Label Stack	Downstream MPLS label stack number.
Status	Return code for the most recent IP SLAs LSP ping operation of the specified equal-cost multipath.

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 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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr mpls-lsp-monitor neighbors** command.

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 9 describes the significant fields shown in the display.

Table 9 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 9 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

operation-number	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.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr mpls-lsp-monitor scan-queue** command.

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 10 describes the significant fields shown in the display.

Table 10 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.
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 ip sla mpls-lsp-monitor summary

To display Border Gateway Protocol (BGP) next hop neighbor and label switched path (LSP) discovery group information for IP Service Level Agreements (SLAs) LSP Health Monitor operations, use the **show ip sla mpls-lsp-monitor summary** command in user EXEC or privileged EXEC mode.

show ip sla mpls-lsp-monitor summary [*operation-number* [**group** [*group-id*]]]

Syntax Description

operation-number	(Optional) Number of the LSP Health Monitor operation for which the details will be displayed.
group *group-id*	(Optional) Specifies the identification number of the LSP discovery group for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Use the **show ip sla mpls-lsp-monitor summary** command if the LSP discovery option is enabled for an LSP Health Monitor operation. This command is not applicable if the LSP discovery option is disabled.

Examples

The following is sample output from the **show ip sla mpls-lsp-monitor summary** *operation-number* command:

```
Router# show ip sla mpls-lsp-monitor summary 1

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

Index Destination Status LPD Group ID Last Operation Time
1 100.1.1.1 up 100001 19:33:37.915 EST Mon Feb 28 2005
2 100.1.1.2 down 100002 19:33:47.915 EST Mon Feb 28 2005
3 100.1.1.3 retry 100003 19:33:57.915 EST Mon Feb 28 2005
4 100.1.1.4 partial 100004 19:34:07.915 EST Mon Feb 28 2005
```

The following is sample output from the **show ip sla mpls-lsp-monitor summary** *operation-number* **group** *group-id* command:

```
Router# show ip sla mpls-lsp-monitor summary 1 group 100001

Group ID - Unique number to identify a LPD group
Lsp-selector - Unique 127/8 address used to identify an LPD.
```

```
Latest operation status - Latest probe status.
Last Operation time - Time when the last operation was attempted.

Group ID Lsp-Selector Status Failures Successes RTT Last Operation Time
100001 127.0.0.13 up 0 78 32 *20:11:37.895 EST Mon Feb 28 2005
100001 127.0.0.15 up 0 78 32 *20:11:37.995 EST Mon Feb 28 2005
100001 127.0.0.16 up 0 78 32 *20:11:38.067 EST Mon Feb 28 2005
100001 127.0.0.26 up 0 78 32 *20:11:38.175 EST Mon Feb 28 2005
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip sla mpls-lsp-monitor summary Field Descriptions

Field	Description
Failures	Number of times the IP SLAs operation for the specified LSP failed to report an RTT value.
Successes	Number of times the IP SLAs operation for the specified LSP successfully reported an RTT value.
RTT	Average round-trip time (in milliseconds) for the specified LSP.

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 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 12 describes the fields shown in the display.

Table 12 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.

Table 12 show mpls discovery vpn Field Descriptions (continued)

Field	Description
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.
in use by	Names of the VPN routing or forwarding instances (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.

timeout (LSP discovery)

To set the amount of time the label switched path (LSP) discovery process for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation waits for a response to its echo request packets, use the **timeout** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

timeout *seconds*

no timeout

Syntax Description

seconds	The amount of time (in seconds) the LSP discovery process waits for a response to its echo request packets. The default value is 5 seconds.

Command Default

5 seconds

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If no response is received for echo request packets sent along a particular LSP within the specified time limit, the LSP is considered to have had an operation failure.

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The timeout value for the echo request packets sent during the LSP discovery process is 4 seconds.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
```

```
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3
action-type trapOnly
```

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.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

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 or IP SLA configuration mode. To return to the default value, use the **no** form of this command.

ttl *time-to-live*

no ttl

Syntax Description

time-to-live	Specifies the maximum hop count for an echo request packet. 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.

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 and IP SLA Monitor Configuration

LSP ping configuration (config-sla-monitor-lspPing)
LSP trace configuration (config-sla-monitor-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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 13). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see Table 14 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 13 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, 12.0(32)SY, 12.2(33)SRB, or later releases	**ip sla**	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, or 12.2(31)SB2	**ip sla monitor**	IP SLA monitor configuration

Table 14 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, 12.0(32)SY, 12.2(31)SB2, 12.2(33)SRB, or later releases	**auto ip sla mpls-lsp-monitor**	Auto IP SLA MPLS configuration

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source Provider Edge (PE) router. The maximum hop count for echo request packets of IP SLAs operations created by LSP Health Monitor operation 1 is set to 200 hops.

```
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
```

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.

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 MPLS configuration mode.

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

Syntax Description

ipsla-vrf-all	(Optional) Specifies that LSP ping operations should be automatically created for all Border Gateway Protocol (BGP) next hop neighbors in use by a VPN routing or forwarding instance (VRF) corresponding to all the Virtual Private Networks (VPNs) in which the originating Provider Edge (PE) router belongs. This option is the default.
vrf *vpn-name*	(Optional) Specifies that LSP ping operations should be automatically created for only those BGP next hop neighbors associated with the specified VPN name.

Command Default

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

Command Modes

Auto IP SLA MPLS configuration (config-auto-ip-sla-mpls)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

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.

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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 Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing or forwarding instances (VRFs) associated with the source 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
 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
```

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.

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 MPLS configuration mode.

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

Syntax Description

ipsla-vrf-all	(Optional) Specifies that LSP traceroute operations should be automatically created for all Border Gateway Protocol (BGP) next hop neighbors in use by a VPN routing or forwarding instance (VRF) corresponding to all the Virtual Private Networks (VPNs) in which the originating Provider Edge (PE) router belongs. This option is the default.
vrf *vpn-name*	(Optional) Specifies that LSP traceroute operations should be automatically created for only those BGP next hop neighbors associated with the specified VPN name.

Command Default

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

Command Modes

Auto IP SLA MPLS configuration (config-auto-ip-sla-mpls)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

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.

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 LSP Health Monitor operation, you must first delete the operation (using the **no auto ip sla mpls-lsp-monitor** global configuration command) and then reconfigure the operation with the new operation type.

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.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, 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.

```
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
```

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.

Feature Information for the LSP Health Monitor

Table 15 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/cfn. An account on Cisco.com is not required.

Note Table 15 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 15 Feature Information for the LSP Health Monitor

Feature Name	Releases	Feature Information
IP SLAs—LSP Health Monitor	12.2(27)SBC, 12.2(28)SB, 12.2(33)SRA	The IP SLAs LSP Health Monitor feature provides the capability to proactively monitor Layer 3 MPLS VPNs.
IP SLAs—LSP Health Monitor with LSP Discovery	12.2(31)SB2	New command line interface (CLI) was implemented to replace the CLI introduced in Cisco IOS Release 12.2(27)SBC and 12.2(28)SB. The LSP discovery capability was added.
IP SLAs—LSP Health Monitor with LSP Discovery	12.2(33)SRB	New command line interface (CLI) was implemented to replace the CLI introduced in Cisco IOS Release 12.2(33)SRA. The LSP discovery capability was added.