

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

Command Default The DSCP value is 0.

Command Modes Auto IP SLA MPLS 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.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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 and forwarding (VRF) instances 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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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 and forwarding (VRF) instances 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.

request-data-size

To set the protocol data size in the payload of a Cisco IOS IP Service Level Agreements (SLAs) operation's request packet, use the **request-data-size** command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, or IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description

<i>bytes</i>	Size (in bytes) of the protocol data in the payload of the request packet of the operation. The range is from 0 to the maximum of the protocol.
--------------	---

Defaults

The default data size will vary depending on the type of IP SLAs operation you are configuring. See the CISCO-RTTMON-MIB documentation for more details.

Command Modes

IP SLA Configuration

DLSw configuration (config-ip-sla-dlsw)
 ICMP echo configuration (config-ip-sla-echo)
 ICMP path echo configuration (config-ip-sla-pathEcho)
 ICMP path jitter configuration (config-ip-sla-pathJitter)
 UDP echo configuration (config-ip-sla-udp)
 UDP jitter configuration (config-ip-sla-jitter)
 VCCV configuration (config-sla-vccv)

Auto IP SLA MPLS Configuration

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

IP SLA Monitor Configuration

DLSw configuration (config-sla-monitor-dlsw)
 ICMP echo configuration (config-sla-monitor-echo)
 ICMP path echo configuration (config-sla-monitor-pathEcho)
 ICMP path jitter configuration (config-sla-monitor-pathJitter)
 UDP echo configuration (config-sla-monitor-udp)
 UDP jitter configuration (config-sla-monitor-jitter)



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
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	The VCCV configuration mode was added.

Usage Guidelines

The **request-data-size** command is also used to set the padding size for the data frame of an IP SLAs Ethernet operation. See the documentation for the **request-data-size** (Ethernet) command for more information.

The **request-data-size** command is supported in IPv4 networks. This command is also supported in IPv6 networks when configuring an IP SLAs operation that supports IPv6 addresses.

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 23](#)). Note that if you are configuring an IP SLAs label switched path (LSP) Health Monitor operation, see [Table 24](#) for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **request-data-size** 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 and the ICMP echo operation type is configured, you would enter the **request-data-size** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 23 *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, 12.2(33)SB, 12.2(33)SXI , or later releases	ip sla	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, 12.2(31)SB2, or 12.2(33)SXH	ip sla monitor	IP SLA monitor configuration

Table 24 *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, 12.2(33)SXH, or later releases	auto ip sla mpls-lsp-monitor	Auto IP SLA MPLS configuration

Examples

The following examples show how to set the request packet size to 40 bytes for IP SLAs ICMP echo operation 3. Note that 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 23](#)).

IP SLA Configuration

This example shows the **request-data-size** command being used in an IPv4 network in ICMP echo configuration mode within IP SLA configuration mode:

```
ip sla 3
 icmp-echo 172.16.1.175
  request-data-size 40
!
ip sla schedule 3 life forever start-time now
```

IP SLA Monitor Configuration

This example shows the **request-data-size** command being used in an IPv4 network in ICMP echo configuration mode within IP SLA monitor configuration mode:

```
ip sla monitor 3
 type echo protocol ipIcmpEcho 172.16.1.175
  request-data-size 40
!
ip sla monitor schedule 3 life forever 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.

request-data-size (Ethernet)

To set the padding size for the data frame of a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the **request-data-size** (Ethernet) command in the appropriate submode of IP SLA configuration or auto IP SLA MPLS configuration mode. To return to the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description	<i>bytes</i>	Padding size (in bytes) for the data frame of the operation. The range is from 0 to the maximum of the protocol.
---------------------------	--------------	--

Defaults The default padding size will vary depending on the type of IP SLAs operation you are configuring. See the CISCO-RTTMON-MIB documentation for more details.

Command Modes	IP SLA Configuration
	Ethernet echo (config-ip-sla-ethernet-echo) Ethernet jitter (config-ip-sla-ethernet-jitter)
	IP SLA Auto Ethernet Configuration
	Ethernet parameters configuration (config-ip-sla-ethernet-params)

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines You must configure the type of Ethernet operation (such as Ethernet ping) before you can configure any of the other parameters of the operation.

Examples The following example shows how to set the padding size to 40 bytes for IP SLAs Ethernet ping operation 3:

```
ip sla 3
  ethernet echo mpid 23 domain testdomain vlan 34
  request-data-size 40
!
ip sla schedule 3 life forever start-time now
```

Related Commands	Command	Description
	auto ip sla ethernet-monitor	Begins configuration for an IP SLAs auto Ethernet operation and enters IP SLA Ethernet monitor configuration mode.
	ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

rtr



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr** command is replaced by the **ip sla monitor** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr** command is replaced by the **ip sla** command. See the **ip sla monitor** and **ip sla** commands for more information.

To begin configuration for a Cisco IOS IP Service Level Agreements (IP SLAs) operation and enter RTR configuration mode, use the **rtr** command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

rtr *operation-number*

no rtr *operation-number*

Syntax Description

<i>operation-number</i>	Operation number used for the identification of the IP SLAs operation you wish to configure.
-------------------------	--

Defaults

No IP SLAs operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).
12.3(14)T	This command was replaced by the ip sla monitor command.
12.2(31)SB2	This command was replaced by the ip sla monitor command.
12.2(33)SRB	This command was replaced by the ip sla command.

Usage Guidelines

The **rtr** command is used to configure Cisco IOS IP Service Level Agreements (IP SLAs) operations. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, you will enter the RTR configuration mode.

IP SLAs allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

After you configure a operation, you must schedule the operation. For information on scheduling a operation, refer to the **rtr schedule** and **rtr group schedule** global configuration commands. You can also optionally set reaction triggers for the operation. For information on reaction triggers, refer to the **rtr reaction-configuration** and **rtr reaction-trigger** global configuration commands.

**Note**

After you schedule an operation, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, you must first delete the IP SLAs operation (using the **no rtr** command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show rtr configuration EXEC** command.

Examples

In the following example, operation 1 is configured to perform end-to-end IP SLAs operations using an SNA LU Type 0 connection with the host name cwbc0a. Only the **type RTR** configuration command is required; all others are optional.

```
rtr 1
  type echo protocol snalu0echoappl cwbc0a
  request-data-size 40
  response-data-size 1440
```

**Note**

If operation 1 already existed and it has not been scheduled, you are placed into RTR configuration mode. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
rtr group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action type options are defined with the ip sla monitor reaction-configuration command.
rtr schedule	Configures the scheduling parameters for a single IP SLAs operation.
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

rtr group schedule



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr group schedule** command is replaced by the **ip sla monitor group schedule** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr group schedule** command is replaced by the **ip sla group schedule** command. See the **ip sla monitor group schedule** and **ip sla group schedule** commands for more information.

To perform group scheduling for Cisco IOS IP Service Level Agreements (IP SLAs) operations, use the **rtr group schedule** command in global configuration mode. To stop the operation and place it in the default state of normal scheduling, use the **no** form of this command.

```
rtr group schedule group-operation-number operation-id-numbers schedule-period
schedule-period-range [ageout seconds] [frequency group-operation-frequency] [life {forever
| seconds}] [start-time {hh:mm[:ss] [month day | day month] | pending | now |
after hh:mm:ss}]
```

```
no rtr group schedule
```

Syntax Description

<i>group-operation-number</i>	Group configuration or group schedule number of the IP SLAs operation to be scheduled. The range is from 0 to 65535.
<i>operation-id-numbers</i>	The list of IP SLAs operation ID numbers in the scheduled operation group. Indicate ranges of operation ID numbers with a hyphen. Individual ID numbers and ranges of ID numbers are delimited by a comma. For example, enter a list of operation ID numbers in any of the following ways: <ul style="list-style-type: none"> 2, 3, 4, 9, 20 10-20, 30-35, 60-70 2, 3, 4, 90-100, 105-115 The <i>operation-id-numbers</i> argument can include a maximum of 125 characters.
schedule-period <i>schedule-period-range</i>	Time (in seconds) for which the IP SLAs operation group is scheduled. The range is from 1 to 604800.
ageout <i>seconds</i>	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 (never ages out).
frequency <i>group-operation-frequency</i>	(Optional) Specifies the number of seconds after which each IP SLAs operation is restarted. If this keyword and argument are specified, the frequency of all operations belonging to the group will be overridden and set to the specified frequency. The range is from 1 to 604800. Note If this keyword and argument are not specified, the frequency for each operation is set to the value specified for the schedule period.
life forever	(Optional) Schedules the operation to run indefinitely.
life <i>seconds</i>	(Optional) Number of seconds the operation actively collects information. The default is 3600 (one hour).

start-time	(Optional) Time when the operation starts collecting information. If the start-time is not specified, no information is collected until the start-time is configured or a trigger occurs that performs a start-time now .
<i>hh:mm[:ss]</i>	(Optional) Specifies an absolute start time using hours, minutes, and (optionally) 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 <i>month</i> and <i>day</i> .
<i>month</i>	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month by using either the full English name or the first three letters of the month.
<i>day</i>	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after <i>hh:mm:ss</i>	(Optional) Indicates that the operation should start <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after this command was entered.

Defaults

The 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
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor group schedule command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the ip sla monitor group schedule command.
12.2(33)SRB	This command was replaced by the ip sla group schedule command.

Usage Guidelines

Though IP SLAs multiple operations scheduling functionality helps in scheduling thousands of operations, you should be cautious while specifying the number of operations, the schedule period, and the operation group frequency to avoid CPU hogging.

For example, consider a scenario where you are scheduling 1 to 780 operations at a schedule period of 60 seconds, the command would be as follows:

rtr group schedule 2 1-780 schedule-period 60 start-now

IP SLAs calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (780 operations divided by 60 seconds, which is 13 operations per second). Operations 1 to 13 in operation group 2 start after 0 seconds, operations 14 to 26 start after 1 second, operations 27 to 40 start after 2 seconds, and the iteration continues until operations 768 to 780 start after 59 seconds. This high value of operations starting at every 1-second interval (especially for jitter operations) can load the CPU to very high values.

The maximum recommended value of operations per second is 6 or 7. This is approximately 350 to 400 operations per minute. This value of 6 or 7 operation per second will be the maximum that does not have any major performance (CPU) impact. However, this value varies from platform to platform. The above value is verified and tested on a Cisco 2600 router.

**Note**

No warning messages will be displayed if IP SLAs multiple operations scheduling leads to a high number of operations starting per second.

When you reboot the router, the IP SLAs multiple operations scheduling functionality schedules the operations in the same order as was done before the reboot. For example, assume the following operation had been scheduled:

rtr group schedule 2 1-20 schedule-period 40 start-time now

Over a range of 40 seconds, 20 operations have to be started (that is, one operation every 2 seconds). After the system reboot, operation 1 will start at t seconds and operation 2 starts at $t+2$ seconds, operation 3 starts at $t+4$ seconds, and so on.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without aborting. However, this functionality skips those IP SLAs operations that are already running or those that are not configured and hence do not exist. The total number of operations will be calculated based on the number of operations specified in the command, irrespective of the number of operations that are missing or already running. The IP SLAs multiple operations scheduling functionality displays a message showing the number of active and missing operations. However, these messages are displayed only if you schedule operations that are not configured or are already running.

Examples

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1:

```
rtr group schedule 1 3, 4, 6-10
```

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1, with a schedule period of 20 seconds:

```
rtr group schedule 1 3, 4, 6-10 schedule-period 20
```

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1, with a schedule period of 20 seconds with start time as now:

```
rtr group schedule 1 3, 4, 6-10 schedule-period 20 start-time now
```

Related Commands

Command	Description
rtr schedule	Enters rtr scheduling mode.
show rtr collection-statistics	Displays the collection details of the IP SLAs operation.

Command	Description
show rtr configuration	Displays the configuration details of the IP SLAs operation.
show rtr operation	Displays the operation details of the IP SLAs operation.

rtr key-chain



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr key-chain** command is replaced by the **ip sla monitor key-chain** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr key-chain** command is replaced by the **ip sla key-chain** command. See the **ip sla monitor key-chain** and **ip sla key-chain** commands for more information.

To enable Cisco IOS IP Service Level Agreements (IP SLAs) control message authentication and specify an MD5 key chain, use the **rtr key-chain** command in global configuration mode. To remove control message authentication, use the **no** form of this command.

rtr key-chain *name*

no rtr key-chain

Syntax Description

<i>name</i>	Name of MD5 key chain.
-------------	------------------------

Defaults

Control message authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor key-chain command.
12.2(31)SB2	This command was replaced by the ip sla monitor key-chain command.
12.2(33)SRB	This command was replaced by the ip sla key-chain command.

Usage Guidelines

The authentication configuration on the IP SLAs source and IP SLAs Responder devices must be the same. In other words, both devices must be configured with the same key chain or both devices must not use authentication.

If the **rtr key-chain** command is entered, at least one key must be added to the specified MD5 key chain in order for MD5 authentication to occur.

Examples

In the following example, the IP SLAs control message uses MD5 authentication, and the key chain name is CSAA. The authentication string for key 1 is csaakey1.

```
rtr key-chain csaa
key chain csaa
key 1
key-string csaakey1
```

Related Commands	Command	Description
	key	Identifies an authentication key on a key chain.
	key chain	Enables authentication for routing protocols and identifies a group of authentication keys.
	key-string (authentication)	Specifies the authentication string for a key.
	rtr	Specifies an IP SLAs operation and enters RTR configuration mode.

rtr logging traps



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr logging traps** command is replaced by the **ip sla monitor logging traps** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr logging traps** command is replaced by the **ip sla logging traps** command. See the **ip sla monitor logging traps** and **ip sla logging traps** commands for more information.

To enable the generation of Simple Network Management Protocol (SNMP) system logging messages specific to Cisco IOS IP Service Level Agreements (SLAs) trap notifications, use the **rtr logging traps** command in global configuration mode. To disable IP SLAs system logging SNMP traps, use the **no** form of this command.

rtr logging traps

no rtr logging traps

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP system logging messages specific to IP SLAs trap notifications are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor logging traps command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the ip sla monitor logging traps command.
12.2(33)SRB	This command was replaced by the ip sla logging traps command.

Usage Guidelines

SNMP trap notifications for IP SLAs can be configured as a triggered action, to be sent when monitored values exceed an upper threshold or fall below a lower threshold, or when a set of defined conditions are met. For example, an SNMP trap can be triggered by five consecutive timeouts during an IP SLAs operation. The sending of SNMP traps is one of the options for triggered actions that can be configured for IP SLAs threshold violations. To configure proactive threshold monitoring parameters for an IP SLAs operation, use the **rtr reaction-configuration** command in global configuration mode.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **snmp-server enable traps rtr** command to enable the sending of IP SLAs SNMP trap notifications.

Examples

The following example shows the configuration of IP SLAs traps to be triggered for round-trip time (RTT) violations and Voice over IP (VoIP) mean opinion score (MOS) violations, and the necessary SNMP configuration for enabling these SNMP logging traps:

```
rtr 1
  type jitter dest-ipaddr 209.165.200.225 dest-port 9234
  !
rtr schedule 1 start now life forever
rtr reaction-configuration 1 react rtt threshold-type immediate threshold-value 3000 2000
action-type trapOnly
rtr reaction-configuration 1 react MOS threshold-type consecutive 4 threshold-value 390
220 action-type trapOnly
!
rtr logging traps
snmp-server enable traps rtr
```

Related Commands

Command	Description
logging on	Controls (enables or disables) system message logging globally.
rtr reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.

rtr low-memory



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr low-memory** command is replaced by the **ip sla monitor low-memory** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr low-memory** command is replaced by the **ip sla low-memory** command. See the **ip sla monitor low-memory** and **ip sla low-memory** commands for more information.

To specify how much unused memory must be available to allow Cisco IOS IP Service Level Agreements (IP SLAs) configuration, use the **rtr low-memory** command in global configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

rtr low-memory *value*

no rtr low-memory

Syntax Description

<i>value</i>	Specifies amount of memory, in bytes, that must be available to configure IP SLAs. The range is from 0 to the maximum amount of free memory bytes available.
--------------	--

Defaults

The default *value* is 25 percent of the memory available on the system.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor low-memory command.
12.2(31)SB2	This command was replaced by the ip sla monitor low-memory command.
12.2(33)SRB	This command was replaced by the ip sla low-memory command.

Usage Guidelines

The **rtr low-memory** command allows the user to specify the amount of memory that IP SLAs can use. If the amount of available free memory falls below the value specified in the **rtr low-memory** command, then you will not be allowed to configure new IP SLAs operations. If this command is not used, the default low-memory value is 25 percent. This means that if 75 percent of system memory has been utilized you will not be able to configure any IP SLAs characteristics.

The value of the **rtr low-memory** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory EXEC** command.

Examples

In the following example, the router is configured so that no less than 2 MB of memory will be free for IP SLAs configuration:

```
rtr low-memory 2000000
```

Related Commands

Command	Description
rtr	Specifies an identification number for an IP SLAs operation and enters RTR configuration mode.
show memory	Displays statistics about memory, including memory-free pool statistics.

rtr mpls-lsp-monitor



Note

Effective with Cisco IOS Releases 12.2(31)SB2 and 12.2(33)SRB, the **rtr mpls-lsp-monitor** command is replaced by the **auto ip sla mpls-lsp-monitor** command. See the **auto ip sla mpls-lsp-monitor** command for more information.

To begin configuration for an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation and enter SAA Multiprotocol Label Switching (MPLS) configuration mode, use the **rtr 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.

rtr mpls-lsp-monitor *operation-number*

no rtr mpls-lsp-monitor *operation-number*

Syntax Description

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

Command Default

No LSP Health Monitor operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the auto ip sla mpls-lsp-monitor command.
12.2(33)SRB	This command was replaced by the auto ip sla 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 **rtr mpls-lsp-monitor schedule** command in global configuration mode. You can also optionally set reaction configuration for the operation (see the **rtr mpls-lsp-monitor reaction-configuration** command).

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

Examples

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

rtr mpls-lsp-monitor

```

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

```

Related Commands

Command	Description
rtr mpls-lsp-monitor reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLAs LSP Health Monitor.
rtr mpls-lsp-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.
show rtr 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.

rtr mpls-lsp-monitor reaction-configuration



Note

Effective with Cisco IOS Releases 12.2(31)SB2 and 12.2(33)SRB, the **rtr mpls-lsp-monitor reaction-configuration** command is replaced by the **auto ip sla mpls-lsp-monitor reaction-configuration** command. See the **auto ip sla mpls-lsp-monitor reaction-configuration** command for more information.

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **rtr 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.

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

```
no rtr mpls-lsp-monitor reaction-configuration operation-number
```

Syntax Description

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

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was replaced by the auto ip sla mpls-lsp-monitor reaction-configuration command.
	12.2(33)SRB	This command was replaced by the auto ip sla mpls-lsp-monitor reaction-configuration command.

Usage Guidelines You can configure the **rtr 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 rtr 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. Use the **rtr 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 rtr 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 BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified by the reaction condition configuration, when three consecutive connection loss or timeout events occur, an SNMP logging trap is sent.

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

Related Commands

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

rtr mpls-lsp-monitor schedule



Note

Effective with Cisco IOS Releases 12.2(31)SB2 and 12.2(33)SRB, the **rtr mpls-lsp-monitor schedule** command is replaced by the **auto ip sla mpls-lsp-monitor schedule** command. See the **auto ip sla mpls-lsp-monitor schedule** command for more information.

To configure the scheduling parameters for an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **rtr 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.

```
rtr 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 rtr mpls-lsp-monitor schedule operation-number
```

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History	Release	Modification
	12.2(27)SBC	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was replaced by the auto ip sla mpls-lsp-monitor schedule command.
	12.2(33)SRB	This command was replaced by the auto ip sla mpls-lsp-monitor schedule command.

Usage Guidelines

After you schedule an LSP Health Monitor operation with the **rtr mpls-lsp-monitor schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no rtr 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 rtr mpls-lsp-monitor configuration** command in EXEC mode.

Examples

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

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

Related Commands

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

rtr reaction-configuration



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr reaction-configuration** command is replaced by the **ip sla monitor reaction-configuration** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr reaction-configuration** command is replaced by the **ip sla reaction-configuration** command. See the **ip sla monitor reaction-configuration** and **ip sla reaction-configuration** commands for more information.

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **rtr reaction-configuration** command in global configuration mode. To clear all threshold monitoring configuration for a specified IP SLAs operation, use the **no** form of this command.

```
rtr reaction-configuration operation-number [react monitored-element] [threshold-type {never
| immediate | consecutive [consecutive-occurrences] | xofy [x-value y-value] | average
[number-of-measurements] }] [threshold-value upper-threshold lower-threshold] [action-type
{none | trapOnly | triggerOnly | trapAndTrigger}]
```

```
no rtr reaction-configuration operation-number
```

Syntax Description

<i>operation-number</i>	Number of the IP SLAs operation to configure for which reactions are to be configured.
react <i>monitored-element</i>	<p>Specifies the element to be monitored for threshold violations. Keyword options for the <i>monitored-element</i> are:</p> <p>connectionLoss—Specifies that a reaction should occur if there is a connection loss for the monitored operation. Thresholds do not apply to this monitored element.</p> <p>jitterAvg—Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold.</p> <p>jitterDSAvg—Specifies that a reaction should occur if the average destination-to-source (DS) jitter value violates the upper threshold or lower threshold.</p> <p>jitterSDAvg—Specifies that a reaction should occur if the average source-to-destination (SD) jitter value violates the upper threshold or lower threshold.</p> <p>mos—Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold.</p>

react <i>monitored-element</i> (continued)	<p>PacketLossDS—Specifies that a reaction should occur if the destination-to-source packet loss value violates the upper threshold or lower threshold.</p> <p>PacketLossSD—Specifies that a reaction should occur if the source-to-destination packet loss value violates the upper threshold or lower threshold.</p> <p>rtt—Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold.</p> <p>timeout—Specifies that a reaction should occur if there is a timeout for the monitored operation. Thresholds do not apply to this monitored element.</p> <p>verifyError—Specifies that a reaction should occur if there is an error verification violation. Thresholds do not apply to this monitored element.</p>
threshold-type never	Do not calculate threshold violations. This is the default threshold-type.
threshold-type immediate	When a threshold violation is met for the monitored element, immediately perform the action defined by action-type .
threshold-type consecutive [<i>consecutive-occurences</i>]	<p>When a threshold violation is met for the monitored element five times in a row, perform the action defined by action-type. The optional <i>consecutive-occurences</i> argument can be used to change the number of consecutive occurrences from the default of 5. The valid range is from 1 to 16.</p> <p>The <i>consecutive-occurences</i> value will appear in the output of the show rtr reaction-configuration command as the “Threshold Count:” value.</p>
threshold-type xofy [<i>x-value y-value</i>]	<p>When a threshold violation is met for the monitored element after some number (x) of violations within some other number (y) of measurements (“x of y”), perform the action defined by action-type. The default is 5 for both <i>x-value</i> and <i>y-value</i> (xofy 5 5). The valid range for each value is from 1 to 16.</p> <p>The <i>x-value</i> value will appear in the output of the show rtr reaction-configuration command as the “Threshold Count:” value, and the <i>y-value</i> will appear as the “Threshold Count2:” value.</p>
threshold-type average [<i>number-of-measurements</i>]	<p>When the average of the last five values for the monitored element exceeds the upper threshold or when the average of the last five values for the monitored element drops below the lower threshold, perform the action defined by action-type. For example, if the upper threshold for react rtt threshold-type average 3 is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be $6000 + 6000 + 5000 = 17000 / 3 = 5667$, thus violating the 5000-ms upper threshold.</p> <p>The default number of 5 averaged measurements can be changed using the optional <i>number-of-measurements</i> argument. The valid range from 1 to 16.</p> <p>This syntax is not available if connectionLoss, timeout, or verifyError is specified as the monitored element, as upper and lower thresholds do not apply to these options.</p>

[threshold-value <i>upper-threshold</i> <i>lower-threshold</i>]	(Optional) Specifies the upper-threshold value and lower-threshold values, for jitterAvg , jitterDSAvg , jitterSDAvg , mos , PacketLossDS , PacketLossSD , and rtt .
	The default upper-threshold value for all monitored elements except mos is 4500, and the default lower-threshold value is 3000.
	For MOS threshold values (react mos), the number is expressed in 3 digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter 320 . The valid range is from 100 (1.00) to 500 (5.00). The default upper-threshold for MOS is 300 (3.00) and the default lower-threshold is 200 (2.00).
action-type <i>option</i>	(Optional) Specify what action or combination of actions the operation performs when you configure connection-loss-enable or timeout-enable , or threshold events occur. For the action-type to occur for threshold events, the threshold-type must be defined to anything other than never . Option can be one of the following keywords:
	<ul style="list-style-type: none"> • none—No action is taken. • trapOnly—Send an SNMP logging trap when the specified violation type occurs for the monitored element. IP SLAs logging traps are enabled using the rtr logging traps command. For SNMP logging traps to be sent, SNMP logging must be enabled using the appropriate SNMP commands, including the snmp-server enable traps syslog command. • triggerOnly—Have one or more target operation's operational state make the transition from "pending" to "active" when the violation conditions are met. The target operations to be triggered are specified using the rtr reaction-trigger command. A target operation will continue until its life expires, as specified by the target operation's configured lifetime value). A triggered target operation must finish its life before it can be triggered again. • trapAndTrigger—Trigger both an SNMP trap and start another IP SLAs operation when the violation conditions are met, as defined in the trapOnly and triggerOnly options above.
	The following SNA NMVT action-type options appear in the command line help, but are no longer valid: nmvtOnly , trapAndNmvt , nmvtAndTrigger , trapNmvtAndTrigger . These SNA NMVT CLI options will be removed in an upcoming release.

Defaults

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.1(1)T	The verify-error-enable optional keyword was added.
	12.3(7)T	<p>This command was enhanced to provide new monitored elements and reaction options. The old syntax of</p> <pre>rtr reaction-configuration <i>operation-number</i> [verify-error-enable] [connection-loss-enable] [timeout-enable] [threshold-falling <i>milliseconds</i>] [threshold-type <i>option</i>] [action-type <i>option</i>]</pre> <p>was replaced by the syntax shown above.</p> <p>Note Configuration of IP SLAs reactions using the old syntax remains available in release 12.3(7)T for backwards compatibility, but support for the old syntax will be removed in an upcoming release.</p> <ul style="list-style-type: none"> • The functionality of the connection-loss-enable keyword was replaced by the react connectionLoss syntax. • The functionality of the timeout-enable keyword was replaced by the react timeout syntax. • The functionality of the verify-error-enable keyword was replaced by the react verifyError syntax. • The functionality of the threshold-falling <i>milliseconds</i> syntax (and the threshold RTR configuration command) was replaced by the threshold-value <i>upper-threshold lower-threshold</i> syntax.
	12.3(14)T	This command was replaced by the ip sla monitor reaction-configuration command.
	12.2(31)SB2	This command was replaced by the ip sla monitor reaction-configuration command.
	12.2(33)SRB	This command was replaced by the ip sla reaction-configuration command.

Usage Guidelines

You can configure the **rtr reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements (for example, configuring thresholds for destination-to-source packet loss and MOS) for the same operation. However, disabling of individual monitored elements is not supported. In other words, the **no rtr 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. Use the **rtr 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 IP SLAs operation, use the **show rtr configuration** command.

Examples

In the following example, IP SLAs operation 10 (a Jitter operation) is configured to send an SNMP logging trap when the MOS value exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
rtr reaction-configuration 10 react mos threshold-type immediate threshold-value 490 250
action-type trapOnly
```

Related Commands	Command	Description
	rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
	rtr logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
	rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the rtr reaction-configuration global configuration command.
	show rtr reaction-configuration	Displays the configured proactive threshold monitoring settings for all IP SLAs operations or a specified operation.
	show rtr reaction-trigger	Displays the configured state of triggered IP SLAs operations.

rtr reaction-trigger



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr reaction-trigger** command is replaced by the **ip sla monitor reaction-trigger** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr reaction-trigger** command is replaced by the **ip sla reaction-trigger** command. See the **ip sla monitor reaction-trigger** and **ip sla reaction-trigger** commands for more information.

To define a second Cisco IOS IP Service Level Agreements (IP SLAs) operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** command, use the **rtr reaction-trigger** command in global configuration mode. To remove the trigger combination, use the **no** form of this command.

```
rtr reaction-trigger operation-number target-operation
```

```
no rtr reaction-trigger operation
```

Syntax Description

<i>operation-number</i>	Number of the operation in the active state that has the action-type set with the rtr reaction-configuration global configuration command.
<i>target-operation</i>	Number of the operation in the pending state that is waiting to be triggered with the rtr global configuration command.

Defaults

No trigger combination is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor reaction-trigger command.
12.2(31)SB2	This command was replaced by the ip sla monitor reaction-trigger command.
12.2(33)SRB	This command was replaced by the ip sla reaction-trigger command.

Usage Guidelines

Triggers are usually used for diagnostics purposes and are not used in normal operation.

Examples

In the following example, the state of operation 1 is changed from pending state to active state when **action-type of** operation 2 occurs:

```
rtr reaction-trigger 2 1
```

Related Commands	Command	Description
	rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
	rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
	rtr schedule	Configures the scheduling parameters for an IP SLAs operation.

rtr reset



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr reset** command is replaced by the **ip sla monitor reset** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr reset** command is replaced by the **ip sla reset** command. See the **ip sla monitor reset** and **ip sla reset** commands for more information.

To perform a shutdown and restart of the Cisco IOS IP Service Level Agreements (SLAs) engine, use the **rtr reset** command in global configuration mode.

rtr reset

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor reset command.
12.2(31)SB2	This command was replaced by the ip sla monitor reset command.
12.2(33)SRB	This command was replaced by the ip sla reset command.

Usage Guidelines

The **rtr reset** command stops all operations, clears IP SLAs configuration information, and returns the IP SLAs feature to the startup condition. This command does not reread the IP SLAs configuration stored in startup-config in NVRAM. You must retype the configuration or load a previously saved configuration file.



Note

The **rtr reset** command does not remove IP SLAs label switched path (LSP) Health Monitor configurations from the running configuration.



Caution

Use the **rtr reset** command only in extreme situations such as the incorrect configuration of a number of operations.

Examples

The following example resets IP SLAs, clearing all stored IP SLAs information and configuration:

```
rtr reset
```

rtr reset**Related Commands**

Command	Description
rtr restart	Restarts a stopped IP SLAs operation.

rtr responder



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr responder** command is replaced by the **ip sla monitor responder** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr responder** command is replaced by the **ip sla responder** command. See the **ip sla monitor responder** and **ip sla responder** commands for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder on a destination (operational target) device, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

rtr responder

no rtr responder

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor responder command.
12.2(31)SB2	This command was replaced by the ip sla monitor responder command.
12.2(33)SRB	This command was replaced by the ip sla responder command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the sending of receiving of IP SLAs Control packets. Enabling the IP SLAs Responder allows the generation of monitoring statistics on the device sending IP SLAs operations.

Examples

The following example enables the IP SLAs Responder:

```
rtr responder
```

Related Commands

Command	Description
rtr responder type tcpConnect	Enables the IP SLAs Responder for TCP Connect operations.
rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

rtr responder type tcpConnect



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr responder type tcpConnect** command is replaced by the **ip sla monitor responder type tcpConnect ipaddress** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr responder type tcpConnect** command is replaced by the **ip sla responder tcp-connect ipaddress** command. See the **ip sla monitor type tcpConnect ipaddress** and **ip sla responder tcp-connect ipaddress** commands for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder for TCP Connect operations, use the **rtr responder type tcpConnect** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

```
rtr responder type tcpConnect ipaddress ip-address port port
```

```
no rtr responder type tcpConnect ipaddress ip-address port port
```

Syntax Description

ipaddress <i>ip-address</i>	(Optional) Specifies the IP address that the operation will be received at.
port <i>port</i>	(Optional) Specifies the port number that the operation will be received on.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(1)T	The ipaddr and port keywords were added.
12.3(14)T	This command was replaced by the ip sla monitor responder type tcpConnect ipaddress command.
12.2(31)SB2	This command was replaced by the ip sla monitor responder type tcpConnect ipaddress command.
12.2(33)SRB	This command was replaced by the ip sla responder tcp-connect ipaddress command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the acceptance and return of TCP Connect operation packets.

Examples

The following example shows how to enable the IP SLAs Responder for TCP connection operations:

```
rtr responder type tcpConnect ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr responder type frame-relay	Enables the IP SLAs Responder for Frame Relay operations.
rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

rtr responder type udpEcho



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr responder type udpEcho** command is replaced by the **ip sla monitor responder type udpEcho ipaddress** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr responder type udpEcho** command is replaced by the **ip sla responder udp-echo ipaddress** command. See the **ip sla monitor type udpEcho ipaddress** and **ip sla responder udp-echo ipaddress** commands for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder for User Datagram Protocol (UDP) Echo or Jitter operations, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

```
rtr responder type udpEcho ipaddress ip-address port port
```

```
no rtr responder type udpEcho ipaddress ip-address port port
```

Syntax Description

ipaddress <i>ip-address</i>	Specifies the IP address that the operation will be received at.
port <i>port</i>	Specifies the port number that the operation will be received on.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.3(14)T	This command was replaced by the ip sla monitor responder type udpEcho ipaddress command.
12.2(31)SB2	This command was replaced by the ip sla monitor responder type udpEcho ipaddress command.
12.2(33)SRB	This command was replaced by the ip sla responder udp-echo ipaddress command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable UPD Echo and Jitter (UDP+) operations on non-native interfaces.

Examples

The following example enables the IP SLAs Responder for Jitter operations:

```
rtr responder type udpEcho ipaddress A.B.C.D port 1
```

Related Commands	Command	Description
	rtr responder	Enables the IP SLAs Responder for non-specific IP SLAs operations.
	rtr responder type frame-relay	Enables the IP SLAs Responder for Frame Relay operations.

rtr restart



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr restart** command is replaced by the **ip sla monitor restart** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr restart** command is replaced by the **ip sla restart** command. See the **ip sla monitor restart** and **ip sla restart** commands for more information.

To restart a Cisco IOS IP Service Level Agreements (IP SLAs) operation, use the **rtr restart** command in global configuration mode.

rtr restart *operation-number*

Syntax Description

<i>operation-number</i>	Number of the IP SLAs operation to restart. IP SLAs allows a maximum of 2000 operations.
-------------------------	--

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).
12.3(14)T	This command was replaced by the ip sla monitor restart command.
12.2(31)SB2	This command was replaced by the ip sla monitor restart command.
12.2(33)SRB	This command was replaced by the ip sla restart command.

Usage Guidelines

To restart an operation, the operation should be in an “active” state (as defined in the **rtr reaction-configuration** command).

IP SLAs allows a maximum of 2000 operations.

This command does not have a **no** form.

Examples

The following example restarts operation 12:

```
rtr restart 12
```

Related Commands

Command	Description
rtr reset	Clears all current IP SLAs statistics and configuration information from the router and resets the IP SLAs engine.

rtr schedule



Note

Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr schedule** command is replaced by the **ip sla monitor schedule** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr schedule** command is replaced by the **ip sla schedule** command. See the **ip sla monitor schedule** and **ip sla schedule** commands for more information.

To configure the scheduling parameters for a Cisco IOS IP Service Level Agreements (IP SLAs) single operation, use the **rtr 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.

```
rtr schedule group-operation-number [life {forever | seconds}] [start-time {hh:mm[:ss]
  [month day | day month] | pending | now | after hh:mm:ss}] [ageout seconds] [recurring]
```

```
no rtr schedule group-operation-number
```

Syntax Description

<i>group-operation-number</i>	Group configuration or group schedule number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life <i>seconds</i>	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time <i>hh:mm[:ss]</i>	Time when the operation starts. Specifies an absolute start time using hour, minute, and (optionally) second. 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 <i>month</i> and <i>day</i> .
<i>month</i>	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month by using either the full English name or the first three letters of the month.
<i>day</i>	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after <i>hh:mm:ss</i>	(Optional) Indicates that the operation should start <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after this command was entered.
ageout <i>seconds</i>	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The after and forever keywords were added.
12.3(8)T	The recurring keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. This integration includes the addition of the recurring keyword.
12.3(14)T	This command was replaced by the ip sla monitor schedule command.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC. This integration includes the addition of the recurring keyword.
12.2(31)SB2	This command was replaced by the ip sla monitor schedule command.
12.2(33)SRB	This command was replaced by the ip sla restart command.

Usage Guidelines

After you schedule the operation with the **rtr schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the **rtr** global configuration command and reenter the configuration information.

If the operation is in a pending state, you can define the conditions under which the operation makes the transition from pending to active with the **rtr reaction-trigger** and **rtr reaction-configuration** global configuration commands. When the operation is in an active state, it immediately begins collecting information.

The following time line shows the age-out process of the operation:

W-----X-----Y-----Z

where:

- W is the time the operation was configured with the **rtr** global configuration command.
- X is the start time or start of life of the operation (that is, when the operation became “active”).
- Y is the end of life as configured with the **rtr schedule** global configuration command (life seconds have counted down to zero).
- Z is the age out of the operation.

Age out starts counting down at W and Y, is suspended between X and Y, and is reset to its configured size at Y.

It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation’s configuration time and start time (X and W) must be less than the age-out seconds.

**Note**

The total RAM required to hold the history and statistics tables is allocated at the time of scheduling the IP SLAs operation. This prevents router memory problems when the router gets heavily loaded and lowers the amount of overhead an IP SLAs operation causes on a router when it is active.

The **recurring** keyword is only supported for scheduling single IP SLAs operations. You cannot schedule multiple IP SLAs operations using the **rtr schedule** command. The **life** value for a recurring IP SLAs operation should be less than one day. The **ageout** value for a recurring operation must be “never” (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the **recurring** option is not specified, the operations are started in the existing normal scheduling mode.

Examples

In the following example, operation 25 begins actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished with its life. When this operation ages out, all configuration information for the operation is removed (that is, the configuration information is no longer in the running-config in RAM).

```
rtr schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

In the following example, operation 1 begins collecting data after a 5-minute delay:

```
rtr schedule 1 start after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
rtr schedule 3 start-time now life forever
```

In the following example, operation 15 begins automatically collecting data every day at 1:30 a.m.:

```
rtr schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr group schedule	Performs group scheduling for IP SLAs operations.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action-type options is defined with the rtr reaction-configuration global configuration command.
show rtr configuration	Displays the configuration details of the IP SLAs operation.

samples-of-history-kept

To set the number of entries kept in the history table per bucket for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **samples-of-history-kept** command in the appropriate submode of IP SLA configuration or IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

samples-of-history-kept *samples*

no samples-of-history-kept

Syntax Description	<i>samples</i>	Number of entries kept in the history table per bucket. The default is 16.
---------------------------	----------------	--

Defaults	16 entries
-----------------	------------

Command Modes	IP SLA Configuration
	ICMP path echo configuration (config-ip-sla-pathEcho)
	IP SLA Monitor Configuration
	ICMP path echo configuration (config-sla-monitor-pathEcho)



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
	11.2	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An IP SLAs operation can collect history and capture statistics. By default, the history for an IP SLAs operation is not collected. If history is collected, each history bucket contains one or more history entries from the operation. When the operation type is ICMP path echo, an entry is created for each hop along the path that the operation takes to reach its destination. The type of entry stored in the history table is controlled by the **filter-for-history** command. The total number of entries stored in the history table is controlled by the combination of the **samples-of-history-kept**, **buckets-of-history-kept**, and **lives-of-history-kept** commands.



Note

This command is supported by the IP SLAs ICMP path echo operation only.

**Note**

Collecting history increases the RAM usage. Collect history only when you think there is a problem in the network.

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 25](#)). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **samples-of-history-kept** command varies depending on the Cisco IOS release you are running (see [Table 25](#)) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP path echo operation type is configured, you would enter the **samples-of-history-kept** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

Table 25 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, 12.2(33)SB, 12.2(33)SXI , or later releases	ip sla	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, 12.2(31)SB2, or 12.2(33)SXH	ip sla monitor	IP SLA monitor configuration

Examples

In the following examples, ten entries are kept in the history table for each of the lives of IP SLAs ICMP path echo operation 1. Note that 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 25](#)).

IP SLA Configuration

```
ip sla 1
  path-Echo 172.16.1.176
  history lives-kept 3
  samples-of-history-kept 10
!
ip sla schedule 1 life forever start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 1
  type pathecho protocol ipIcmpEcho 172.16.1.176
  lives-of-history-kept 3
  samples-of-history-kept 10
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during the lifetime of the IP SLAs operation.
filter-for-history	Defines the type of information kept in the history table for the IP SLAs operation.
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.
lives-of-history-kept	Sets the number of lives maintained in the history table for the IP SLAs operation.

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

Command Default Scan interval is 240 minutes.

Command Modes Auto IP SLA MPLS 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.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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.



Note

The default interval of time that BGP neighbor statistics are updated is different for the IP SLAs LSP Health Monitor database and the BGP next hop neighbor discovery database. Use the **scan-interval** command to set the timer for the IP SLAs LSP Health Monitor database. Use the **mpls discovery vpn interval** command to set the timer for the BGP next hop neighbor discovery database.

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 and forwarding (VRF) instances 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	<i>minutes</i>	The amount of time (in minutes) after which the LSP discovery process can restart. The default is 1.
---------------------------	----------------	--

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 redisccovery 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 redisccovery 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 and forwarding (VRF) instances associated with the source Provider Edge (PE) router. The LSP redisccovery 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, IP SLA configuration, or IP SLA monitor configuration mode. To disable the secondary frequency, use the **no** form of this command.

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

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

Syntax Description

both	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way connection loss or one-way timeout is detected.
connection-loss	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way connection loss is detected.
timeout	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way timeout is detected.
<i>frequency</i>	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)
VCCV configuration (config-ip-sla-vecv)

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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	Support for MPLS Pseudo-Wire Emulation Edge-to-Edge (PWE3) services via Virtual Circuit Connectivity Verification (VCCV) was added.
12.2(33)SB	Support for MPLS Pseudo-Wire Emulation Edge-to-Edge (PWE3) services via Virtual Circuit Connectivity Verification (VCCV) was added.

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 label switched path (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 26](#)). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see [Table 27](#) 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 26 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, 12.2(33)SB, or later releases	ip sla	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, 12.2(31)SB2, or 12.2(33)SXH	ip sla monitor	IP SLA monitor configuration

Table 27 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, 12.2(33)SXH, 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 and forwarding (VRF) instances 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	<i>seconds</i>	The amount of time (in seconds) an LSP Health Monitor operation waits for a response to its LSP discovery request. The default is 120.
---------------------------	----------------	--

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 and forwarding (VRF) instances 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.