Cisco IOS IP SLAs Command Reference

November 8, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS IP SLAs Command Reference

Cisco IOS IP SLAs Commands

access-list (epl-disc)

To add a list of discovered endpoints to an auto IP Service Level Agreements (SLAs) endpoint list, use the **access-list** command in IP SLA endpoint-list auto-discovery configuration mode. To remove the list, use the **no** form of this command.

access-list {*standard-list-number* | *expanded-list-number*}

no access-list

Syntax Description

standard-list-number	Unique identifier of list. Range is from 1 to 99.
expanded-list-number	Unique identifier of list. Range is from 1300 to 1999.

Command Default

No access list is specified in the auto IP SLAs endpoint list being configured.

Command Modes

IP SLA endpoint-list auto-discovery configuration (config-epl-disc)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command assigns a name to a list of discovered IP addresses of IP SLAs destination devices and Cisco IOS IP SLAs Responder endpoints and adds the list to the auto IP SLAs endpoint list being configured.

Before you use this command, you must use the **discover** command in IP SLA endpoint-list configuration mode to build the list of endpoints on target Cisco devices.

To apply an endpoint list to an IP SLAs auto-measure group, use the **destination** command in IP SLA auto-measure group configuration mode.

Examples

The following example shows how to configure an endpoint list using the auto discovery method:

```
Router(config)# ip sla auto discovery
Router(config)# ip sla auto endpoint-list type ip autolist
Router(config-epl)# discover port 5000
Router(config-epl-disc)# access-list 3
Router(config-epl-disc)# end
Router# show ip sla auto endpoint-list
Endpoint-list Name: autolist
    Description:
    Auto Discover Parameters
        Destination Port: 5000
        Access-list: 3
        Ageout: 3600    Measurement-retry: 3

    5 endpoints are discovered for autolist
```

Related Commands

Command	Description
destination (am-group)	Specifies an IP SLAs endpoint list for an IP SLAs auto-measure group.
discover (epl)	Builds a list of endpoints.
ip sla auto discovery	Enables auto discovery in Cisco IP SLAs Engine 3.0.
ip sla responder auto-register	Enables the Cisco device or Cisco IP SLAs Responder to automatically register with the source upon configuration
show ip sla auto endpoint-list	Displays the configuration including default values of auto IP SLAs endpoint lists.

access-list (IP SLA)

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

access-list *access-list-number*

no access-list *access-list-number*

Syntax Description

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

Command Default

No access list is specified.

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Standard IP access lists can be configured (using the **access-list** [IP standard] command in global configuration mode) to restrict the number of IP SLAs operations that are automatically created by the IP SLAs LSP Health Monitor. When the IP SLAs access list parameter is configured, the list of Border Gateway Protocol (BGP) next hop neighbors discovered by the LSP Health Monitor is filtered based on the conditions defined by the associated standard IP access list. In other words, the LSP Health Monitor will automatically create IP SLAs operations only for those BGP next hop neighbors with source addresses that satisfy the criteria permitted by the standard IP access list.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. Standard IP access list 10 is specified to restrict the number of IP SLAs operations to be created by LSP Health Monitor operation 1.

```
!Configure standard IP access list in global configuration mode
access-list 10 permit 10.10.10.8
!
```

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

Related Commands

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

ageout

To add an ageout timer to an auto IP Service Level Agreements (SLAs) scheduler or endpoint list, use the **ageout** command in IP SLA auto-measure schedule configuration or IP SLA endpoint-list auto-discovery configuration mode. To remove the timer, use the **no** form of this command.

ageout *seconds*

no ageout

Syntax Description

seconds	Length of time to keep an entry in memory, in seconds. Range is from 0 to 2073600. Default is 0.

Command Default

The entry is never saved in memory.

Command Modes

IP SLA auto-measure schedule configuration (config-am-schedule)
IP SLA endpoint-list auto-discovery configuration (config-epl-disc)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the length of time an entry is kept in memory when either the operation or destination is inactive from the default (0) to the specified number, after which the entry is deleted from memory.

An operation can age out before it executes. To ensure that this does not happen, the difference between the time that the IP SLA auto-measure group is configured and the time at which the operation becomes active must be less than the value of the ageout timer.

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

Examples

The following example shows how to configure an auto IP SLAs scheduler that will cause an auto IP SLAs operation to actively collect data at 3:00 p.m. on April 5. The operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished its life. When the operation ages out, all configuration information for the operation is removed from the running configuration in RAM.

```
Router(config)# ip sla auto schedule apr5
Router(config-am-schedule)# ageout 43200
Router(config-am-schedule)# frequency 70
Router(config-am-schedule)# life 43200
Router(config-am-schedule)# probe-interval 1500
Router(config-am-schedule)# start-time 15:00 apr 5
```

```
Router(config-am-schedule)# end
Router#
Router# show ip sla auto schedule apr5
Group sched-id: apr5
    Probe Interval (ms) : 1500
    Group operation frequency (sec): 70
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: P15:00 apr 5
    Life (sec): 43200
    Entry Ageout (sec): 43200
Router#
```

Related Commands

Command	Description
frequency	Specifies how often an auto IP SLAs operation will repeat once it is started.
life	Specifies length of time that an auto IP SLAs operation will run.
probe-interval	Specifies interval for staggering the start times of auto IP SLAs operations
show ip sla auto schedule	Displays configuration including default values of auto IP SLAs schedulers.
start-time	Specifies when an auto IP SLAs operation will start running.

auto ip sla mpls-lsp-monitor

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

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

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

Syntax Description

operation-number	Number used for the identification of the LSP Health Monitor operation you want to configure.

Command Default

No LSP Health Monitor operation is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Entering this command automatically enables the **mpls discovery vpn next-hop** command.

After you configure an LSP Health Monitor operation, you must schedule the operation. To schedule an LSP Health Monitor operation, use the **auto ip sla mpls-lsp-monitor schedule** command in global configuration mode. You can also optionally set reaction configuration for the operation (see the **auto ip sla mpls-lsp-monitor reaction-configuration** command).

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router.

```
mpls discovery vpn interval 60
```

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

Related Commands

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

auto ip sla mpls-lsp-monitor reaction-configuration

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **auto ip sla mpls-lsp-monitor reaction-configuration** command in global configuration mode. To clear all threshold monitoring configuration for a specified LSP Health Monitor operation, use the **no** form of this command.

LSP Health Monitor Without LSP Discovery

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

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

LSP Health Monitor with LSP Discovery

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

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

Syntax Description

operation-number	Number of the LSP Health Monitor operation for which reactions are to be configured.
react connectionLoss	Enables monitoring of one-way connection loss events.
react timeout	Enables monitoring of one-way timeout events.
action-type *option*	(Optional) Specifies what action is performed when threshold events occur. If the **threshold-type never** keywords are defined, the **action-type** keyword is disabled. The *option* argument can be one of the following keywords: • **none**—No action is taken. This option is the default value. • **trapOnly**—SNMP trap notification is sent.
threshold-type consecutive [*occurrences*]	(Optional) When a threshold violation for the monitored element (such as a timeout) are met consecutively for a specified number of times, perform the action defined by the **action-type** keyword. The default number of 5 consecutive occurrences can be changed using the *occurrences* argument. The range is from 1 to 16.
threshold-type immediate	(Optional) When a threshold violation for the monitored element (such as a timeout) are met, immediately perform the action defined by the **action-type** keyword.
threshold-type never	(Optional) Do not calculate threshold violations. This option is the default threshold type.
lpd	(Optional) Specifies the LSP discovery option.
lpd-group	(Optional) Enables monitoring of LSP discovery group status changes.

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

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss or timeout events occur, an SNMP trap notification is sent.

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

auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
ip sla monitor logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.
snmp-server enable traps rtr	Enables the sending of IP SLAs SNMP trap notifications.

auto ip sla mpls-lsp-monitor reset

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

auto ip sla mpls-lsp-monitor reset [**lpd** *group-number*]

Syntax Description

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

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

auto ip sla mpls-lsp-monitor schedule

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. The schedule period for LSP Health Monitor operation 1 is set to 60 seconds and the operation is scheduled to start immediately.

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

Related Commands

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

buckets-of-history-kept

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **buckets-of-history-kept** command is replaced by the **history buckets-kept** command. See the **history buckets-kept** command for more information.

To set the number of history buckets that are kept during the lifetime of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **buckets-of-history-kept** command in the appropriate submode of IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

buckets-of-history-kept *size*

no buckets-of-history-kept

Syntax Description

size	Number of history buckets kept during the lifetime of the operation. The default is 50.

Defaults

50 buckets

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **history buckets-kept** command.
12.2(33)SRB	This command was replaced by the **history buckets-kept** command.
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)SB	This command was replaced by the **history buckets-kept** command.
12.2(33)SXI	This command was replaced by the **history buckets-kept** command.

Usage Guidelines

Each time IP SLAs starts an operation, a new bucket is created until the number of history buckets matches the specified size or the operation's lifetime expires. History buckets do not wrap (that is, the oldest information is not replaced by newer information). The operation's lifetime is defined by the **ip sla monitor schedule** global configuration command.

Note The **buckets-of-history-kept** command does not support the IP SLAs User Datagram Protocol (UDP) jitter operation.

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

Note 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.

Examples

The following example shows how to configure IP SLAs ICMP echo operation 1 to keep 25 history buckets during the operation lifetime.

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.161.21
 buckets-of-history-kept 25
 lives-of-history-kept 1
!
ip sla monitor schedule 1 start-time now life forever
```

Related Commands

Command	Description
filter-for-history	Defines the type of information kept in the history table for the IP SLAs operation.
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.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the IP SLAs operation.

clock-tolerance ntp oneway

To set the acceptable Network Time Protocol (NTP) clock synchronization tolerance for a one-way Cisco IOS IP Service Level Agreements (SLAs) operation measurement, use the **clock-tolerance ntp oneway** command in the UDP jitter submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

clock-tolerance ntp oneway {**absolute** *value* | **percent** *value*}

no clock-tolerance ntp oneway

Syntax Description

absolute *value*	Sets the NTP synchronization tolerance value to an absolute number, in microseconds. The range is from 0 to 100000.
percent *value*	Sets the NTP synchronization tolerance value as a percentage of the one-way IP SLAs operation delay measurement. The range is from 0 to 100. The NTP clock synchronization tolerance is set to 0 percent by default.

Command Default

The NTP clock synchronization tolerance is set to 0 percent.

Command Modes

IP SLA Configuration

UDP jitter configuration (config-ip-sla-jitter)

IP SLA Monitor Configuration

UDP jitter configuration (config-sla-monitor-jitter)

IP SLA Template Parameters Configuration

UDP jitter configuration (config-udp-jtr-params)

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
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(1)T	This command was modified. The IP SLA template parameters configuration mode was added.

Usage Guidelines

The **precision microseconds** command must be configured before the **clock-tolerance ntp oneway** command is used.

Note This command is supported by the IP SLAs User Datagram Protocol (UDP) jitter operation only.

If the NTP running state is true and the total offset (sum of the offset for the sender and responder) is within the specified tolerance value (defined using the **clock-tolerance ntp oneway** command) of a one-way IP SLAs operation measurement for all the packets in a stream, the NTP synchronization status is determined to be synchronized. If these conditions are not met, the status is determined to be not synchronized.

The following guidelines apply to the displayed output:

- If the NTP synchronization status is determined to be synchronized, the one-way IP SLAs delay measurement values will be displayed.
- If the NTP synchronization status is determined to be not synchronized, the one-way values will be zero.
- The total number of operational packets that are not synchronized will be tracked during the collection period and reported.

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 1). 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 **clock-tolerance ntp oneway** command varies depending on the Cisco IOS release you are running (see Table 1) and the operation type configured.

If you are using auto IP SLAs in Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **clock-tolerance ntp oneway** command.

Table 1 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Examples

The following examples show how to enable microsecond precision, configure the NTP synchronization offset tolerance to 10 percent, and set the packet priority to high for IP SLAs UDP jitter 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 1).

IP SLA Configuration

```
ip sla 1
 udp-jitter 205.199.199.2 dest-port 9006
 precision microseconds
 clock-tolerance ntp oneway percent 10
 probe-packet priority high
 frequency 300
!
ip sla schedule 1 life forever start-time after 00:00:06
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type jitter dest-ipaddr 205.199.199.2 dest-port 9006
 precision microseconds
 clock-tolerance ntp oneway percent 10
 probe-packet priority high
 frequency 300
!
ip sla monitor schedule 1 life forever start-time after 00:00:06
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip udp-jitter 1
Router(config-udp-jtr-tplt)# parameters
Router(config-udp-jtr-params)# precision microseconds
Router(config-udp-jtr-params)# clock-tolerance ntp oneway percent 10
Router(config-udp-jtr-params)# operation-packet high
Router(config-udp-jtr-params)# end
Router#
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: 1
Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: usec       Operation packet priority: high
        NTP Sync Tolerance: 10 percent
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

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

codec (tplt)

To configure codec in an auto IP Service Level Agreements (SLAs) operation template for a User Datagram Protocol (UDP) jitter operation that returns VoIP scores, use the **codec** command in UDP jitter submode of the IP SLA template configuration mode.

codec *codec-type* [**advantage-factor** *value*] [**codec-numpackets** *number-of-packets*] [**codec-interval** *milliseconds*] [**codec-size** *number-of-bytes*]

Syntax Description

codec-type	The following codec-type keywords are valid: • **g711alaw**—The G.711 a-law codec (64 kbps transmission) • **g711ulaw**—The G.711 mu-law codec (64 kbps transmission) • **g729a**—The G.729A codec (8 kbps transmission)
advantage-factor	(Optional) Specifies expectation factor to be used for ICPIF calculations.
value	Range is from 0 to 20. Default is 0. For recommended values, see Table 3.
codec-numpackets	(Optional) Specifies number of packets to be transmitted per operation.
number-of-packets	Range is from 1 to 60000. Default is 1000.
codec-interval	(Optional) Specifies interval between packets in operation.
milliseconds	Length of interval, in milliseconds (ms). Range is from 1 to 60000. Default is 20.
codec-size	(Optional) Specifies number of bytes in each packet transmitted.
number-of-bytes	Range is from 16 to 1500. Default varies by codec. For default values, see Table 2.

Defaults

A codec is not configured in the auto IP SLAs operation template being configured.

Command Modes

IP SLA UDP jitter template configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command configures the codec in an auto IP SLAs operation template for a UDP jitter operation and generates ICPIF and MOS scores, based on the specified codec type.

The specified *codec-type* should match the encoding algorithm being used for VoIP transmissions.

You must configure the type of auto 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.

A UDP jitter operation computes statistics by sending *n* UDP packets, each of size *s*, sent *t* msec apart, from a given source router to a given target router, at a given frequency *f*. Based on the type of codec you configure for the operation, the number of packets (*n*), the size of each payload (*s*), the interpacket time interval (*t*), and the operational frequency (*f*) are auto-configured with default values or you can manually configure these parameters using the keyword and argument combinations in this command.

Note You should not specify values for the interval, size, and number of packet options unless you have a specific reason to override the defaults; for example, to approximate a different codec.

Table 2 lists the default values for each parameter by codec.

Table 2 Default UDP Jitter Operation Parameters by Codec

Codec	Default Number of Packets (*n*); [codec-numpackets]	Packet Payload (*s*) [codec-size][1]	Default Interval Between Packets (*t*) [codec-interval]	Frequency of Operations (*f*)
G.711 mu-law (g711ulaw)	1000	160 bytes	20 ms	Once every 60 seconds
G.711 a-law (g711alaw)	1000	160 bytes	20 ms	Once every 60 seconds
G.729A (g729a)	1000	20 bytes	20 ms	Once every 60 seconds

1. The actual data size of each request packet will contain an additional 12 bytes of Real-Time Transport Protocol (RTP) header data in order to simulate the RTP/UDP/IP/Layer 2 protocol stack.

The **advantage-factor** *value* keyword and argument allow you to specify an access Advantage Factor, also known as the Expectation Factor. Table 3, adapted from ITU-T Rec. G.113, defines a set of provisional maximum values for Advantage Factors in terms of the service provided.

Table 3 Advantage Factor Recommended Maximum Values

Communication Service	Maximum Value of Advantage/ Expectation Factor (*A*):
Conventional wire line (land line)	0
Mobility (cellular connections) within a building	5
Mobility within a geographical area or moving within a vehicle	10
Access to hard-to-reach location; for example, via multihop satellite connections	20

These values are only suggestions. To be meaningful, the Advantage/Expectation factor (*A*) and its selected value in a specific application should be used consistently in any planning model you adopt. However, the values in Table 3 should be considered as the absolute upper limits for *A*. The default Advantage/Expectation factor for UDP jitter operations is always zero.

Examples

In the following example, an auto IP SLAs operation template for a UDP jitter (codec) operation is configured to use the default characteristics of the G.711 a-law codec, which means the operation will consist of 1000 packets, each of 172 bytes (160 plus 12 header bytes), sent 20 ms apart. The default value for the Advantage Factor and operations frequency is used.

```
Router(config)# ip slas auto template type ip udp-jitter voip
Router(config-tplt)# codec g711alaw
Router(config-tplt)# end
Router# show ip sla auto template type ip udp-jitter voip
IP SLAs Auto Template: voip
    Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Verify Data: false
        Timeout: 5000           Threshold: 5000
        Codec: g711alaw Number of packets: 1000
        Interval: 20    Payload size: 16        Advantage factor: 0
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
ip sla auto template	Enters IP SLA template configuration mode for defining an auto IP SLAs operation template.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.

control

To enable or disable control messages in an auto IP Service Level Agreements (SLAs) operation template, use the **control** command in the appropriate submode of the IP SLA template configuration mode. To return to the default value, use the **no** form of this command.

control {**enable** | **disable**}

no control

Syntax Description

enable	Sends IP SLAs control messages to the IP SLAs Responder. This is the default.
disable	Does not send IP SLAs control messages between the source and the IP SLAs Responder.

Command Default

IP SLAs control messaging is enabled.

Command Modes

IP SLA Template Configuration

TCP connect template configuration (config-tplt-tcp-conn)
UDP echo template configuration (config-tplt-udp-ech)
UDP jitter template configuration (config-tplt-udp-jtr)

Command HistoryTC

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command disables or enables control messages for an auto IP SLAs operation. Prior to sending an operation packet to the destination router, IP SLAs sends a control message to the IP SLAs Responder to enable the destination port. Control protocol is required when the target device is a Cisco router that does not natively provide the UDP or TCP Connect service.

If you disable control, you must define the IP address of the source for the Cisco IOS IP SLAs Responder by using the **ip sla responder tcp-connect ipaddress** or **ip sla responder udp-echo ipaddress** command on the destination device.

The **no** form of this command returns the configuration to the default (enabled). If control is already enabled (default), the **no** form of this command has no affect.

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.

Examples

The following example shows how to configure an auto IP SLA operation template for a TCP connect operation from Router 2 (10.1.1.1) to host device1. In this example, the control protocol is disabled. Auto IP SLAs uses the control protocol to notify the IP SLAs Responder to enable the target port temporarily. This action allows the Responder to reply to the TCP Connect operation. Because the control is disabled, you must configure the IP address of the source for the endpoint.

Router (Destination)

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Roter1(config)# ip sla responder ipaddress 10.1.1.1 port 23
Router(config)# exit
Router# show running-config
.
.
.
!
ip sla responder
 ip sla responder ipaddress 10.1.1.1 port 23
```

Router (Source)

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip sla auto template type ip tcp-connect 6
Router(config-tplt-tcp-conn)# control disable
Router(config-tplt-tcp-conn)# tos 128
Router(config-tplt-tcp-conn)# exit
Router# show running-config
.
.
.
ip sla auto template type ip tcp-connect 6
 control disable
 tos 128
```

Related Commands

Command	Description
ip sla auto template	Enters IP SLA template configuration mode for defining an auto IP SLAs operation template.
ip sla responder tcp-connect ipaddress	Defines the IP address of the source for the Cisco IOS IP SLAs Responder for TCP connect operations.
ip sla responder udp-echo ipaddress	Defines the IP address of the source for the Cisco IOS IP SLAs Responder for UDP echo or jitter operations.
show ip sla auto template	Display configuration including default values of auto IP SLAs operation templates.

cos

To set the class of service (CoS) for a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the **cos** command in the appropriate submode of IP SLA configuration or IP SLA Ethernet monitor configuration mode. To return to the default value, use the **no** form of this command.

cos *cos-value*

no cos

Syntax Description

cos-value	Class of service value. The range is from 0 to 7. The default is 0.

Command Default

The class of service value for the IP SLAs Ethernet operation is set to 0.

Command Modes

IP SLA configuration

Ethernet echo configuration (config-ip-sla-ethernet-echo)
Ethernet jitter configuration (config-ip-sla-ethernet-jitter)

IP SLA Ethernet monitor configuration

Ethernet parameters configuration (config-ip-sla-ethernet-params)

Note The configuration mode varies depending on the operation type configured. See the "Usage Guidelines" section for more information.

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 IP SLAs operation (such as Ethernet ping) before you can configure any of the other parameters of the operation.

The configuration mode for the **cos** command varies depending on the operation type configured. For example, if you are running Cisco IOS Release 12.2(33)SRB and the Ethernet ping operation type is configured using the **ethernet echo mpid** command in IP SLA configuration mode, you would enter the **cos** command in Ethernet echo configuration mode (config-ip-sla-ethernet-echo).

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using an IP SLAs auto Ethernet operation. In this example, operation 10 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance

endpoints in the domain named testdomain and VLAN identification number 34. The class of service for each Ethernet ping operation is set to 3. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss events occur, a Simple Network Management Protocol (SNMP) trap notification should be sent. The schedule period for operation 10 is 60 seconds, and the operation is scheduled to start immediately.

```
ip sla ethernet-monitor 10
 type echo domain testdomain vlan 34
 cos 3
!
ip sla ethernet-monitor reaction-configuration 10 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

Related Commands

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

data-pattern

To specify the data pattern in a Cisco IOS IP Service Level Agreements (SLAs) operation to test for data corruption, use the **data pattern** command in the appropriate submode of IP SLA configuration or IP SLA monitor configuration mode. To remove the data pattern specification, use the **no** form of this command.

data-pattern *hex-pattern*

no data-pattern *hex-pattern*

Syntax Description

hex-pattern	Hexadecimal string to use for monitoring the specified operation.

Defaults

The default *hex-pattern* is ABCD.

Command Modes

IP SLA Configuration

UDP echo configuration (config-ip-sla-udp)

IP SLA Monitor Configuration

UDP echo configuration (config-sla-monitor-udp)

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
12.1(1)T	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

The **data-pattern** command allows users to specify an alphanumeric character string to verify that operation payload does not get corrupted in either direction (source-to-destination [SD] or destination-to-source [DS]).

Note The **data-pattern** command is supported by the IP SLAs User Datagram Protocol (UDP) echo operation only.

This command is supported in IPv4 networks and in IPv6 networks.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see Table 4). 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 **data-pattern** command varies depending on the Cisco IOS release you are running (see Table 4) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the UDP echo operation type is configured, you would enter the **data-pattern** command in UDP echo configuration mode (config-sla-monitor-udp) within IP SLA monitor configuration mode.

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

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T, 12.0(32)SY, 12.2(33)SRB, 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

The following examples show how to specify 1234ABCD5678 as the data pattern. 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 4).

The examples show the **data-pattern** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 1
 udp-echo 10.0.54.205 dest-port 101
 data-pattern 1234ABCD5678
!
ip sla schedule 1 life forever start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type udpEcho dest-ipaddr 10.0.54.205 dest-port 101
 data-pattern 1234ABCD5678
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
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.

delete-scan-factor

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

delete-scan-factor *factor*

no delete-scan-factor

Syntax Description

factor	Number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.

Command Default

The default scan factor is 1. In other words, each time the LSP Health Monitor checks the scan queue for updates, it deletes IP SLAs operations for BGP next hop neighbors that are no longer valid.

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

Note If the scan factor is set to 0, IP SLAs operations will not be automatically deleted by the LSP Health Monitor. This configuration is not recommended.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with

the source Provider Edge (PE) router. The delete scan factor is set to 2. In other words, every other time the LSP Health Monitor checks the scan queue for updates, it deletes IP SLAs operations for BGP next hop neighbors that are no longer valid.

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

Related Commands

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

description (IP SLA)

To add a description to the configuration of an IP Service Level Agreements (SLAs) auto-measure group, auto IP SLAs operation template, or auto IP SLAs endpoint list, use the **description** command in IP SLA auto-measure group configuration, IP SLA endpoint-list configuration, or appropriate submode of IP SLA template configuration mode. To remove the description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	String of 1 to 64 ASCII characters.

Command Default

No description is added to configuration.

Command Modes

IP SLA Configuration

IP SLA auto-measure group (config-am-group)
IP SLA endpoint-list (config-epl)

IP SLA Template Configuration

ICMP echo configuration (config-tplt-icmp-ech)
ICMP jitter configuration (config-tplt-icmp-jtr)
TCP connect configuration (config-tplt-tcp-conn)
UDP echo configuration (config-tplt-udp-ech)
UDP jitter configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command adds descriptive text to the configuration of an IP SLAs auto-measure group, auto IP SLAs operation template, or auto IP SLAs endpoint list. The description appears in the **show** command output and does not affect the operation of the template.

Examples

The following example shows how to configure this command for an auto IP SLAs operation template:

```
Router(config)# ip sla auto template type ip icmp-jitter 1
Router(config-tplt-icmp-jtr)# description default oper temp for icmp jitter
Router# end
Router# show ip sla auto template type ip icmp-jitter
IP SLAs Auto Template: 1
    Measure Type: icmp-jitter
    Description: default oper temp for icmp jitter
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
```

```
Operation Parameters:
    Number of Packets: 10   Inter packet interval: 20
    Timeout: 5000           Threshold: 5000
Statistics Aggregation option:
    Hours of statistics kept: 2
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

Related Commands

Command	Description
show ip sla auto group	Displays configuration including default values of IP SLAs auto-measure groups.
show ip sla auto endpoint-list	Displays configuration including default values of auto IP SLAs endpoint lists.
show ip sla auto schedule	Displays configuration including default values of auto IP SLAs schedulers.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.

destination (am-group)

To add an auto IP Service Level Agreements (SLAs) endpoint list to the configuration of an IP SLAs auto-measure group, use the **destination** command in IP SLA auto-measure group configuration mode. To remove the endpoint list from the group configuration, use the **no** form of this command.

destination *template-name*

no destination

Syntax Description

template-name	Name of an already-configured endpoint list.

Command Default

No endpoints are defined for the IP SLAs auto-measure group being configured.

Command Modes

IP SLA auto-measure group configuration (config-am-grp)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command specifies an auto IP SLAs endpoint list as a reference for the IP SLAs auto-measure group being configured. An endpoint list contains IP addresses for IP SLAs endpoints.

Only one auto IP SLAs endpoint list can be specified for each IP SLAs auto-measure group. Each endpoint list can be referenced by more than one group.

To change the auto IP SLAs endpoint list in the configuration of an existing auto-measure group, first use the **no** form of this command to remove the endpoint list from the group configuration and then reconfigure the group with a different endpoint list.

To create an auto IP SLAs endpoint list, use the **ip sla auto endpoint-list** command.

Examples

The following example shows how to add an auto IP SLAs endpoint list to the configuration of an IP SLAs auto-measure group:

```
Router(config)# ip sla auto group type ip 1
Router(config-am-grp)# destination 1
Router(config-am-grp)# schedule 1
Router(config-am-grp)# end
Router#
Router# show ip sla auto group
Group Name: 1
    Description:
    Activation Trigger: Immediate
    Destination: 1
    Schedule: 1

IP SLAs Auto Template: default
    Measure Type: icmp-jitter
```

```
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None

IP SLAs auto-generated operations of group 1
    no operation created
```

Related Commands

Command	Description
ip sla auto endpoint-list	Enters IP SLA endpoint-list configuration mode for creating an auto IP SLAs endpoint list.

dhcp (IP SLA)

To configure a Cisco IOS IP Service Level Agreements (SLAs) Dynamic Host Configuration Protocol (DHCP) operation, use the **dhcp** command in IP SLA configuration mode.

dhcp {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**option-82** [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**subnet-mask** *subnet-mask*]]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
option-82	(Optional) Specifies DHCP option 82 for the destination DHCP server.
circuit-id *circuit-id*	(Optional) Specifies the circuit ID in hexadecimal.
remote-id *remote-id*	(Optional) Specifies the remote ID in hexadecimal.
subnet-mask *subnet-mask*	(Optional) Specifies the subnet mask IP address. The default subnet mask is 255.255.255.0.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type dhcp** command.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type dhcp** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type dhcp** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type dhcp** command.

Usage Guidelines

If the source IP address is configured, then packets will be sent with that source address.

You may configure the **ip dhcp-server** global configuration command to identify the DHCP server that the DHCP operation will measure. If the target IP address is configured, then only that device will be measured. If the **ip dhcp-server** command is not configured and the target IP address is not configured, then DHCP discover packets will be sent on every available IP interface.

Option 82 is called the Relay Agent Information option and is inserted by the DHCP relay agent when client-originated DHCP packets are forwarded to a DHCP server. Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. The initial suboptions are defined for a relay agent that is colocated in a public circuit access unit. These suboptions are as follows: a circuit ID for the incoming circuit, a remote ID that provides a trusted identifier for the remote high-speed modem, and a subnet mask designation for the logical IP subnet from which the relay agent received the client DHCP packet.

Note If an odd number of characters are specified for the circuit ID, a zero will be added to the end of the string.

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

Examples

In the following example, IP SLAs operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3:

```
ip sla 4
 dhcp option-82 circuit-id 10005A6F1234
ip dhcp-server 172.16.20.3
!
ip sla schedule 4 start-time now
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

discover (epl)

To enter IP SLA endpoint-list auto-discovery configuration mode for building a list of destination IP addresses for Cisco routing devices or Cisco IP Service Level Agreements (SLAs) Responders, use the **discover** command in IP SLA endpoint-list configuration mode. To remove the list, use the **no** form of this command.

discover [**port** *port*]

no discover [**port** *port*]

Syntax Description

port	(Optional) Specifies port on source IP SLAs device.
port	Port number. Range is from 1 to 65535. Default is 5000.

Command Default

No destination IP addresses are identified.

Command Modes

IP SLA endpoint-list configuration (config-epl)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command discovers and builds a list of destination IP addresses to be added to an endpoint list for IP SLAs auto-measure groups.

Before using this command, use the **ip sla auto discovery** command to enable auto-discovery.

Before using this command, use the **ip sla responder auto-register** command on the destination Cisco device to enable endpoints to register with source upon configuration.

Destination IP addresses can either be automatically discovered by using this command or manually configured using the **ip-address** command. If you use this command to build an endpoint list, you cannot use the **ip-address** command to manually add or remove IP addresses in an endpoint list.

To add the discovered list of destination IP addresses to the endpoint list being configured, use the **access-list** command in IP SLA endpoint-list auto-discovery configuration mode.

Examples

The following example shows how to configure an endpoint list using the auto discovery method:

Destination Router

```
Router(config)# ip sla responder auto-register 10.1.1.25
Router(config)#
```

Source Router

```
Router(config)# ip sla auto discovery
Router(config)# ip sla auto endpoint-list type ip autolist
```

```
Router(config-epl)# discover port 5000
Router(config-epl-disc)# access-list 3
Router(config-epl-disc)# end
Router# show ip sla auto endpoint-list
Endpoint-list Name: autolist
    Description:
    Auto Discover Parameters
        Destination Port: 5000
        Access-list: 3
        Ageout: 3600    Measurement-retry: 3
.
.
.
```

Related Commands

Command	Description
access-list	Adds a list of discovered endpoints to an auto IP SLAs endpoint list.
ip sla auto discovery	Enables IP SLAs auto discovery for auto IP SLAs in Cisco IOS IP SLAs Engine 3.0.
ip sla responder auto-register	Configures a Cisco IP SLAs Responder to automatically register with the source.
show ip sla auto discovery	Displays the status of IP SLAs auto discovery and the configuration of auto IP SLAs endpoint lists configured using auto discovery.
show ip sla auto endpoint-list	Displays the configuration including default values of auto IP SLAs endpoint lists.

distributions-of-statistics-kept

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **distributions-of-statistics-kept** command is replaced by the **history distributions-of-statistics-kept** command. See the **history distributions-of-statistics-kept** command for more information.

To set the number of statistics distributions kept per hop during a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **distributions-of-statistics-kept** command in the appropriate submode of IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

distributions-of-statistics-kept *size*

no distributions-of-statistics-kept

Syntax Description

size	Number of statistics distributions kept per hop. The default is 1 distribution.

Defaults

1 distribution

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **history distributions-of-statistics-kept** command.
12.2(33)SRB	This command was replaced by the **history distributions-of-statistics-kept** command.
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.

Release	Modification
12.2(33)SB	This command was replaced by the **history distributions-of-statistics-kept** command.
12.2(33)SXI	This command was replaced by the **history distributions-of-statistics-kept** command.

Usage Guidelines

In most situations, you do not need to change the number of statistics distributions kept or the time interval for each distribution. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network. To set the statistics distributions interval, use the **statistics-distribution-interval** command.

When the number of distributions reaches the size specified, no further distribution-based information is stored.

For the IP SLAs Internet Control Message Protocol (ICMP) path echo operation, the amount of router memory required to maintain the distribution statistics table is based on multiplying all of the values set by the following four commands:

- **distributions-of-statistics-kept**
- **hops-of-statistics-kept**
- **paths-of-statistics-kept**
- **hours-of-statistics-kept**

The general equation used to calculate the memory requirement to maintain the distribution statistics table for an ICMP path echo operation is as follows:
Memory allocation = (160 bytes) * (**distributions-of-statistics-kept** *size*) * (**hops-of-statistics-kept** *size*) * (**paths-of-statistics-kept** *size*) * (**hours-of-statistics-kept** *hours*)

Note To avoid significant impact on router memory, careful consideration should be used when configuring the **distributions-of-statistics-kept**, **hops-of-statistics-kept**, **paths-of-statistics-kept**, and **hours-of-statistics-kept** commands.

Note 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.

Examples

The following example shows how to set the statistics distribution to 5 and the distribution interval to 10 ms for IP SLAs ICMP echo operation 1. Consequently, the first distribution will contain statistics from 0 to 9 ms, the second distribution will contain statistics from 10 to 19 ms, the third distribution will contain statistics from 20 to 29 ms, the fourth distribution will contain statistics from 30 to 39 ms, and the fifth distribution will contain statistics from 40 ms to infinity.

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.161.21
 distributions-of-statistics-kept 5
 statistics-distribution-interval 10
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the IP SLAs operation.

dlsw peer-ipaddr

To configure a Cisco IOS IP Service Level Agreements (SLAs) Data Link Switching Plus (DLSw+) operation, use the **dlsw peer-ipaddr** command in IP SLA configuration mode.

dlsw peer-ipaddr *ip-address*

Syntax Description

ip-address	IP address of the peer destination.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type dlsw peer-ipaddr** command.

Usage Guidelines

To configure an IP SLAs DLSw+ operation, the DLSw+ feature must be configured on the local and target routers.

For DLSw+ operations, the default request packet data size is 0 bytes (use the **request-data-size** command to modify this value) and the default amount of time the operation waits for a response from the request packet is 30 seconds (use the **timeout** command to modify this value).

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

Examples

In the following example, IP SLAs operation number 10 is configured as a DLSw+ operation enabled for remote peer IP address 172.21.27.11. The data size is 15 bytes:

```
ip sla 10
 dlsw peer-ipaddr 172.21.27.11
 request-data-size 15
!
ip sla schedule 4 start-time now
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
request-data-size	Sets the protocol data size in the payload of the IP SLAs operation's request packet.
show dlsw peers	Displays DLSw peer information.

dns (IP SLA)

To configure a Cisco IOS IP Service Level Agreements (SLAs) Domain Name System (DNS) operation, use the **dns** command in IP SLA configuration mode.

dns {*destination-ip-address* | *destination-hostname*} **name-server** *ip-address* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
name-server *ip-address*	Specifies the IP address of the DNS server.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type dns target-addr** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type dns target-addr** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type dns target-addr** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type dns target-addr** command.

Usage Guidelines

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

Examples

In the following example, IP SLAs operation 7 is configured as a DNS operation using the target IP address 172.20.2.132:

```
ip sla 7
```

```
 dns host1 name-server 172.20.2.132
!
ip sla schedule 7 start-time now
```

Related Commands

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

enhanced-history

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **enhanced-history** command is replaced by the **history enhanced** command. See the **history enhanced** command for more information.

To enable enhanced history gathering for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **enhanced-history** command in the appropriate submode of IP SLA monitor configuration mode.

enhanced-history [**interval** *seconds*] [**buckets** *number-of-buckets*]

Syntax Description

interval *seconds*	(Optional) Number of seconds that enhanced history should be gathered in each bucket. When this time expires, enhanced history statistics are gathered in a new bucket. The default is 900 (15 minutes).
buckets *number-of-buckets*	(Optional) Number of history buckets that should be retained in system memory. When this number is reached, statistic gathering for the operation ends. The default is 100.

Defaults

900 seconds and 100 buckets

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
12.2(11)T	This command was introduced.
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.
12.4(4)T	This command was replaced by the **history enhanced** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was replaced by the **history enhanced** command.

Release	Modification
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)SB	This command was replaced by the **history enhanced** command.
12.2(33)SXI	This command was replaced by the **history enhanced** command.

Usage Guidelines

Performance statistics are stored in "buckets" that separate the accumulated data. Each bucket consists of data accumulated over the specified time interval.

Note 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.

Examples

In the following example, Internet Control Message Protocol (ICMP) echo operation 3 is configured with the standard enhanced history characteristics.

```
ip sla monitor 3
 type echo protocol ipIcmpEcho 172.16.1.175
 enhanced-history interval 900 buckets 100
!
ip sla monitor schedule 3 start-time now life forever
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
show ip sla monitor enhanced-history collection-statistics	Displays data for all collected history buckets for the specified IP SLAs operation, with data for each bucket shown individually.
show ip sla monitor enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.

ethernet echo mpid

To manually configure an individual Cisco IOS IP Service Level Agreements (SLAs) Ethernet ping operation, use the **ethernet echo mpid** command in IP SLA configuration mode.

ethernet echo mpid *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*}

Syntax Description

mp-id	Maintenance endpoint identification number.
domain *domain-name*	Specifies the name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
evc *evc-id*	Specifies the Ethernet Virtual Circuit (EVC) identification name.
port	Enables port level statistical measurements for two directly connected maintenance endpoints (MEPs).
vlan *vlan-id*	Specifies the VLAN identification number.

Command Default

No IP SLAs Ethernet ping operation is configured.

Command Modes

IP SLA configuration (config-ip-sla)

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)SRD	The **evc** *evc-id* keyword and argument were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. The **port** keyword was added.

Usage Guidelines

Unlike the EVC and VLAN statistical measurements, the port level measurement is performed at the physical layer level and does not cross a bridge boundary.

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

Examples

The following example shows how to configure an IP SLAs Ethernet ping operation. In this example, the maintenance endpoint identification number is 23, the maintenance domain name is testdomain, and the VLAN identification number is 34. Operation 1 is scheduled to start immediately.

```
ip sla 1
 ethernet echo mpid 23 domain testdomain vlan 34
!
```

```
ip sla schedule 1 start-time now
```

Related Commands

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

ethernet jitter mpid

To manually configure an individual Cisco IOS IP Service Level Agreements (SLAs) Ethernet jitter operation, use the **ethernet jitter mpid** command in IP SLA configuration mode.

ethernet jitter mpid *mp-id* **domain** *domain-name* {**evc** *evc-id* | **port** | **vlan** *vlan-id*} [**interval** *interframe-interval*] [**num-frames** *frames-number*]

Syntax Description

mp-id	Maintenance endpoint identification number.
domain *domain-name*	Specifies the name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
evc *evc-id*	Specifies the Ethernet Virtual Circuit (EVC) identification name.
vlan *vlan-id*	Specifies the VLAN identification number.
interval *interframe-interval*	(Optional) Specifies the interframe interval (in milliseconds). The default is 20.
num-frames *frames-number*	(Optional) Specifies the number of frames to be sent. The default is 10.

Command Default

No IP SLAs Ethernet jitter operation is configured.

Command Modes

IP SLA configuration (config-ip-sla)

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)SRD	The **evc** *evc-id* keyword and argument were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was modified. The **port** keyword was added.

Usage Guidelines

Unlike the EVC and VLAN statistical measurements, the port level measurement is performed at the physical layer level and does not cross a bridge boundary.

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

Examples

The following example shows how to configure an IP SLAs Ethernet jitter operation. In this example, the maintenance endpoint identification number is 23, the maintenance domain name is testdomain, the VLAN identification number is 34, the interframe interval is 20 ms, and the number of frames to be sent is 30. Operation 2 is scheduled to start immediately.

```
ip sla 2
 ethernet jitter mpid 23 domain testdomain vlan 34 interval 20 num-frames 30
!
ip sla schedule 2 start-time now
```

Related Commands

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

exp (IP SLA)

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

exp *exp-bits*

no exp

Syntax Description

exp-bits	Specifies the experimental field value in the header for an echo request packet. The range is from 0 to 7. The default is 0.

Command Default

The experimental field value is set to 0.

Command Modes

Auto IP SLA MPLS Configuration

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

IP SLA Configuration and IP SLA Monitor Configuration

LSP ping configuration (config-sla-monitor-lspPing)
LSP trace configuration (config-sla-monitor-lspTrace)
VCCV configuration (config-sla-vccv)

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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

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 5). Note that if you are configuring an IP SLAs label switched path (LSP) Health Monitor operation, see Table 6 for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation.

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

Table 5 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 6 Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T, 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 experimental field value for each IP SLAs operations created by LSP Health Monitor operation 1 is set to 5.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
 exp 5
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
```

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

Related Commands

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

filter-for-history

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **filter-for-history** command is replaced by the **history filter** command. See the **history filter** command for more information.

To define the type of information kept in the history table for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **filter-for-history** command in the appropriate submode of IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

filter-for-history {**none** | **all** | **overThreshold** | **failures**}

no filter-for-history {**none** | **all** | **overThreshold** | **failures**}

Syntax Description

none	No history kept. This is the default.
all	All operations attempted are kept in the history table.
overThreshold	Only packets that are over the threshold are kept in the history table.
failures	Only packets that fail for any reason are kept in the history table.

Defaults

No IP SLAs history is kept for an operation.

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **history filter** command.
12.2(33)SRB	This command was replaced by the **history filter** command.
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)SB	This command was replaced by the **history filter** command.
12.2(33)SXI	This command was replaced by the **history filter** command.

Usage Guidelines

Use the **filter-for-history** command to control what gets stored in the history table for an IP SLAs operation. To control how much history gets saved in the history table, use the **lives-of-history-kept**, **buckets-of-history-kept**, and the **samples-of-history-kept** commands.

Note The **filter-for-history** command does not support the IP SLAs User Datagram Protocol (UDP) jitter operation.

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

Note 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.

Examples

In the following example, only operation packets that fail are kept in the history table.

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.161.21
 lives-of-history-kept 1
 filter-for-history failures
!
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.
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.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the IP SLAs operation.

flow-label (IP SLA)

To define the flow label field in the IPv6 header of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **flow-label** (IP SLA) 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.

flow-label *number*

no flow-label

Syntax Description

number	Value in the flow label field of the IPv6 header. The range is from 0 to 1048575 (or FFFFF hexadecimal). This value can be preceded by "0x" to indicate hexadecimal notation. The default value is 0.

Defaults

The default flow label value is 0.

Command Modes

ICMP echo configuration (config-ip-sla-echo)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)

Note The configuration mode varies depending on the operation type configured.

Command History

Release	Modification
12.2(33)SRC	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.

Usage Guidelines

The flow label value is stored in a a 20-bit field in the IPv6 packet header and is used by a source to label packets of a flow.

A flow label value of zero is used to indicate packets that are not part of any flow.

When the flow label is defined for an operation, the IP SLAs Responder will reflect the flow-label value it receives.

Note This command is applicable only to IPv6 networks.

To display the flow label value for all Cisco IOS IP SLAs operations or a specified operation, use the **show ip sla configuration** command.

Examples

In the following example, IP SLAs operation 1 is configured as an Internet Control Message Protocol (ICMP) echo operation with destination IPv6 address 2001:DB8:100::1. The value in the flow label field of the IPv6 header is set to 0x1B669.

```
ip sla 1
 icmp-echo 2001:DB8:100::1
 flow-label 0x1B669
!
ip sla schedule 1 start-time now
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
show ip sla configuration	Displays configuration values including all defaults for all Cisco IOS IP SLAs operations or a specified operation.

force-explicit-null

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

force-explicit-null

no force-explicit-null

Syntax Description

This command has no arguments or keywords.

Command Default

An explicit null label is not added.

Command Modes

Auto IP SLA MPLS Configuration

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

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. Support for this command in MPLS label switched path (LSP) discovery parameters configuration mode was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 PE router. In this example, an explicit null label will be added to all the echo request packets of IP SLAs operations created by LSP Health Monitor operation 1.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
```

```
 force-explicit-null
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type
consecutive 3 action-type trapOnly
ip sla logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

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

frequency (am-schedule)

To set the frequency characteristic in an auto IP Service Level Agreements (SLAs) scheduler for restarting auto IP SLAs operations, use the **frequency** command in IP SLA auto-measure schedule configuration mode. To return to the default value, use the **no** form of this command.

frequency {*seconds* | **range** *random-frequency-range*}

no frequency

Syntax Description

seconds	Length of time before an operation repeats, in seconds (sec). Range is from 0 to 604800. Default is 60.
range	Specifies frequencies at which auto IP SLAs operations that share the same schedule will restart are chosen randomly within the specified frequency range. Default is disabled.
random-frequency-range	Lower and upper limits of the range, in seconds, and separated by a hyphen (-), such as 80-100. The hyphen (-) is required.

Command Default

Auto IP SLAs operations restart every 60 sec.

Command Modes

IP SLA auto-measure schedule configuration (config-am-schedule)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the value of frequency in an auto IP SLAs scheduler from the default (every 60 sec) to the specified value. The frequency characteristic determines how often an operation in an IP SLAs auto-measure group will repeat once it is started.

Use the **probe-interval** command to configure the interval between the start time of one operation and the start time of the next operation being controlled by the same auto IP SLAs scheduler.

Random Scheduler

The random scheduler option provides the capability to schedule auto IP SLAs operations that share the same scheduler to begin at random intervals over a specified duration of time. The random scheduler option is disabled by default.

To enable the random scheduler option, you must configure the **range** *random-frequency-range* keyword and argument combination. Auto IP SLAs operations being controlled by a random scheduler restart at uniformly distributed random frequencies within the specified frequency range. The following guidelines apply for setting the random frequency range:

- The starting value of the range should be greater than the timeout value of the operations controlled by the scheduler being configured.

- The starting value of the frequency range should be greater than the schedule period (amount of time for which the operations are scheduled). This guideline ensures that the same operation does not get scheduled more than once within the schedule period.

The following guidelines apply if the random scheduler option is enabled:

- The individual operations being controlled by the same auto IP SLAs scheduler will be uniformly distributed to begin at random intervals over the schedule period.
- The operations being controlled by the same auto IP SLAs scheduler restart at uniformly distributed random frequencies within the specified frequency range.
- The minimum interval between the start of each operation being controlled by the same auto IP SLAs scheduler is 100 ms (0.1 sec).
- Only one operation can be scheduled to begin at any given time. If the random scheduler option is disabled, multiple operations can begin at the same time.
- The first operation will always begin at 0 ms of the schedule period.
- The order in which each operation in a multioperation schedule begins is random.

Multioperation Scheduling

Note A multioperation schedule is created by specifying the same auto IP SLA scheduler for two or more IP SLA auto-measure groups.

The following guidelines apply when you add or delete an operation from an existing multioperation schedule by modifying the configuration of an IP SLAs auto-measure group to add or remove the auto IP SLAs scheduler:

- If two or more operations are added after the multioperation schedule has started, then the start times of the newly added operations will be uniformly distributed based on a time interval that was calculated prior to the addition of the new operations. If two or more operations are added before the multioperation schedule has started, then the time interval is recalculated based on both the existing and newly added operations.
- If an operation is added to a multioperation schedule in which the random scheduler option is enabled, then the start time and frequency of the newly added operation will be randomly chosen within the specified parameters.
- If an operation is added to a multioperation schedule in which the existing operations have aged out or the lifetimes of the existing operations have ended, the newly added operation will start and remain active for the amount of time specified by the multioperation schedule.
- If an active operation is deleted, then the operation will stop collecting information and become inactive.

Examples

The following example shows how to configure an auto IP SLAs scheduler that will cause an auto IP SLAs operation to actively collect data at 3:00 p.m. on April 5. The operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished its life. When the operation ages out, all configuration information for the operation is removed from the running configuration in RAM.

```
Router(config)# ip sla auto schedule apr5
Router(config-am-schedule)# ageout 43200
Router(config-am-schedule)# frequency 70
Router(config-am-schedule)# life 43200
Router(config-am-schedule)# probe-interval 1500
```

```
Router(config-am-schedule)# start-time 15:00 apr 5
Router(config-am-schedule)# end
Router# show ip sla auto schedule apr5
Group sched-id: apr5
    Probe Interval (ms) : 1500
    Group operation frequency (sec): 70
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: P15:00 apr 5
    Life (sec): 43200
    Entry Ageout (sec): 43200
```

The following example shows how to schedule auto IP SLAs operations 3, 4, and 6 using multioperation scheduling. In this example, the operations are scheduled to begin at equal intervals over a schedule period of 20 seconds. The first operation (or set of operations) is scheduled to start immediately.

```
Router(config)# ip sla auto schedule multi
Router(config-am-schedule)# probe-interval 20
Router(config-am-schedule)# start-time now
Router(config-am-schedule)# end
Router#
Router# show ip sla auto schedule multi
Group sched-id: multi
    Probe Interval (ms) : 20
    Group operation frequency (sec): 60
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: Now
    Life (sec): 3600
    Entry Ageout (sec): never
Router#configure terminal
Router(config)# ip sla auto group type ip icmp-echo 3
Router(config-am-group)# template 3
Router(config-am-group)# schedule multi
Router(config-am-group)# destination 3
Router(config-am-group)# exit
Router(config)# ip sla auto group type ip icmp-echo 4
Router(config-am-group)# template 4
Router(config-am-group)# schedule multi
Router(config-am-group)# destination 4
Router(config-am-group)# exit
Router(config)# ip sla auto group type ip icmp-echo 6
Router(config-am-group)# template 6
Router(config-am-group)# schedule multi
Router(config-am-group)# destination 6
Router(config-am-group)# exit
Router(config)#
```

Related Commands

Command	Description
probe-interval	Specifies interval for staggering the start times of auto IP SLAs operations
show ip sla auto schedule	Displays configuration including default values of auto IP SLAs schedulers.

frequency (IP SLA)

To set the rate at which a specified IP Service Level Agreements (SLAs) operation repeats, use the **frequency** (IP SLA) 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.

frequency *seconds*

no frequency

Syntax Description

seconds	Number of seconds between the IP SLAs operations. The default is 60.

Defaults

60 seconds

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

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.
12.2(33)SRB	The Ethernet echo and Ethernet jitter configuration modes were added.
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 following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	The Ethernet echo and Ethernet jitter configuration modes were added.

Usage Guidelines

A single IP SLAs operation will repeat at a given frequency for the lifetime of the operation. For example, a User Datagram Protocol (UDP) jitter operation with a frequency of 60 sends a collection of data packets (simulated network traffic) once every 60 seconds, for the lifetime of the operation. The default simulated traffic for a UDP jitter operation consists of ten packets sent 20 milliseconds apart. This "payload" is sent when the operation is started, then is sent again 60 seconds later.

If an individual IP SLAs operation takes longer to execute than the specified frequency value, a statistics counter called "busy" is incremented rather than immediately repeating the operation.

Consider the following guidelines before configuring the **frequency** (IP SLA), **timeout** (IP SLA), and **threshold** (IP SLA) commands. For the IP SLAs UDP jitter operation, the following guidelines are recommended:

- (**frequency** *seconds*) > ((**timeout** *milliseconds*) + N)
- (**timeout** *milliseconds*) > (**threshold** *milliseconds*)

where N = (**num-packets** *number-of-packets*) * (**interval** *interpacket-interval*). Use the **udp-jitter** command to configure the **num-packets** *number-of-packets* and **interval** *interpacket-interval* values.

For all other IP SLAs operations, the following configuration guideline is recommended:

(**frequency** *seconds*) > (**timeout** *milliseconds*) > (**threshold** *milliseconds*)

Note We recommend that you do not set the frequency value to less than 60 seconds because the potential overhead from numerous active operations could significantly affect network performance.

The **frequency** (IP SLA) 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 7). 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 **frequency** (IP SLA) command varies depending on the Cisco IOS release you are running (see Table 7) 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 **frequency** (IP SLA) command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 7 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

The following examples show how to configure an IP SLAs ICMP echo operation (operation 10) to repeat every 90 seconds. 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 7).

IP SLA Configuration

This example shows the **frequency** (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA configuration mode:

```
ip sla 10
 icmp-echo 172.16.1.175
 frequency 90
!
ip sla schedule 10 life 300 start-time after 00:05:00
```

IP SLA Monitor Configuration

This example shows the frequency (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA monitor configuration mode:

```
ip sla monitor 10
 type echo protocol ipIcmpEcho 172.16.1.175
 frequency 90
!
ip sla monitor schedule 10 life 300 start-time after 00:05:00
```

Related Commands

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

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
timeout (IP SLA)	Sets the amount of time the IP SLAs operation waits for a response from its request packet.

ftp get

To configure a Cisco IOS IP Service Level Agreements (SLAs) File Transfer Protocol (FTP) GET operation, use the **ftp get** command in IP SLA configuration mode.

ftp get *url* [**source-ip** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**}

Syntax Description

url	URL location information for the file to be retrieved.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
mode {**passive** | **active**}	(Optional) Specifies the FTP transfer mode as either passive or active. The default is passive transfer mode.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type ftp operation get url** command.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type ftp operation get url** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type ftp operation get url** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type ftp operation get url** command.

Usage Guidelines

The *url* argument must be in one of the following formats:

- ftp://username:password@host/filename
- ftp://host/filename

If the username and password are not specified, the defaults are anonymous and test, respectively.

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

Examples

In the following example, an FTP operation is configured. User1 is the username and password1 is the password; host1 is the host and file1 is the filename.

```
ip sla 3
 ftp get ftp://user1:password1@host1/file1
!
ip sla schedule 3 start-time now
```

Related Commands

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

history buckets-kept

To set the number of history buckets that are kept during the lifetime of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **history buckets-kept** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

history buckets-kept *size*

no history buckets-kept

Syntax Description

size	Number of history buckets kept during the lifetime of the operation. The default is 50.

Command Default

The default number of buckets kept is 50 buckets.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **buckets-of-history-kept** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **buckets-of-history-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **buckets-of-history-kept** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **buckets-of-history-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, TCP connect, and UDP echo configuration submodes in IP SLA template parameters configuration mode were added.

Usage Guidelines

Each time IP SLAs starts an operation, a new bucket is created until the number of history buckets matches the specified size or the lifetime of the operation expires. History buckets do not wrap.

To define the lifetime of an IP SLAs operation, use the **ip sla schedule** global configuration command. To define the lifetime of an auto IP SLAs operation template in Cisco IP SLAs Engine 3.0, use the **life** command in IP SLAs auto-measure schedule configuration mode.

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

The **history buckets-kept** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

By default, the history for an IP SLAs operation is not collected. If history is collected, each bucket contains one or more history entries from the operation. When the operation type is Internet Control Message Protocol (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 **history filter** command.

The total number of entries stored in the history table is controlled by the combination of the **samples-of-history-kept**, **history buckets-kept**, and **history lives-kept** commands.

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

Examples

The following example shows how to configure an ICMP echo operation to keep 25 history buckets during the operation lifetime. The example shows the **history buckets-kept** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla schedule 1 start-time now life forever
ip sla 1
 icmp-echo 172.16.161.21
 history buckets-kept 25
```

```
 history lives-kept 1
!
ip sla schedule 1 start-time now life forever
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# history buckets-kept 25
Router(config-icmp-ech-params)# end
Router# show ip sla auto template type ip icmp-echo 1
IP SLAs Auto Template: 1
    Measure Type: icmp-echo
.
.
.
Statistics Aggregation option:
        Hours of statistics kept: 5
    History options:
        History filter: none
        Max number of history records kept: 25
        Lives of history kept: 1
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
history filter	Defines the type of information kept in the history table for the IP SLAs operation.
history lives-kept	Sets the number of lives maintained 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 auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
life	Specifies the lifetime characteristic in an auto IP SLAs scheduler
samples-of-history-kept	Sets the number of entries kept in the history table per bucket.

history distributions-of-statistics-kept

To set the number of statistics distributions kept per hop during a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **history distributions-of-statistics-kept** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

history distributions-of-statistics-kept *size*

no history distributions-of-statistics-kept

Syntax Description

size	Number of statistics distributions kept per hop. The default is 1.

Command Default

The default is 1 distribution.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
ICMP jitter configuration (config-icmp-jtr-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **distributions-of-statistics-kept** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.

Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **distributions-of-statistics-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **distributions-of-statistics-kept** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **distributions-of-statistics-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, ICMP jitter, TCP connect, UDP echo, and UDP jitter configuration submodes of IP SLA template parameters configuration mode were added.

Usage Guidelines

In most situations, you do not need to change the number of statistics distributions kept or the time interval for each distribution. Change these parameters only when distributions are needed, for example, when performing statistical modeling of your network.

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

To set the statistics distributions interval, use the **history statistics-distribution-interval** command.

When the number of distributions reaches the size specified, no further distribution-based information is stored.

The **history distributions-of-statistics-kept** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

For the IP SLAs Internet Control Message Protocol (ICMP) path echo operation, the amount of router memory required to maintain the distribution statistics table is based on multiplying all of the values set by the following four commands:

- **history distributions-of-statistics-kept**
- **hops-of-statistics-kept**
- **paths-of-statistics-kept**
- **history hours-of-statistics-kept**

The general equation used to calculate the memory requirement to maintain the distribution statistics table for an ICMP path echo operation is as follows:
Memory allocation = (160 bytes) * (**history distributions-of-statistics-kept** *size*) * (**hops-of-statistics-kept** *size*) * (**paths-of-statistics-kept** *size*) * (**history hours-of-statistics-kept** *hours*)

Note To avoid significant impact on router memory, careful consideration should be used when configuring the **history distributions-of-statistics-kept**, **hops-of-statistics-kept**, **paths-of-statistics-kept**, and **history hours-of-statistics-kept** commands.

Examples

In the following examples, the statistics distribution is set to five and the distribution interval is set to 10 ms for an ICMP echo operation. Consequently, the first distribution will contain statistics from 0 to 9 ms, the second distribution will contain statistics from 10 to 19 ms, the third distribution will contain statistics from 20 to 29 ms, the fourth distribution will contain statistics from 30 to 39 ms, and the fifth distribution will contain statistics from 40 ms to infinity. The examples show the **history distributions-of-statistics-kept** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 1
 icmp-echo 172.16.161.21
 history distributions-of-statistics-kept 5
 history statistics-distribution-interval 10
!
ip sla schedule 1 life forever start-time now
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# history distributions-of-statistics-kept 5
Router(config-icmp-ech-params)# history statistics-distribution-interval 10
Router(config-icmp-ech-params)# end
Router# show ip sla auto template type ip icmp-echo 1
IP SLAs Auto Template: 1
    Measure Type: icmp-echo (control enabled)
    Description:
.
.
.
Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 10
        Max number of distributions buckets: 5
```

Related Commands

Command	Description
history hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
history statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the IP SLAs operation.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

Command	Description
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.

history enhanced

To enable enhanced history gathering for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **history enhanced** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode.

history enhanced [**interval** *seconds*] [**buckets** *number-of-buckets*]

Syntax Description

interval *seconds*	(Optional) Number of seconds (sec) that enhanced history should be gathered in each bucket. When this time expires, enhanced history statistics are gathered in a new bucket. The default is 900 (15 minutes).
buckets *number-of-buckets*	(Optional) Number of history buckets that should be retained in system memory. When this number is reached, statistic gathering for the operation ends. The default is 100.

Command Default

Enhanced history gathering is disabled.

Syntax Description

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **enhanced-history** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.

Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **enhanced-history** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **enhanced-history** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **enhanced-history** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, TCP connect, UDP echo, and UDP jitter configuration submodes in IP SLA template parameters configuration mode were added.

Usage Guidelines

This command enables enhanced history for the IP SLAs operation.

Performance statistics are stored in buckets that separate the accumulated data. Each bucket consists of data accumulated over the specified time interval. When the interval expires, history statistics are gathered in a new bucket. When the specified number of buckets is reached, statistic gathering for the operation ends.

By default, IP SLAs maintains two hours of aggregated statistics for each operation. Value from each operation cycle is aggregated with the previously available data within a given hour. The Enhanced History feature in IP SLAs allows for the aggregation interval to be shorter than one hour.

The **history enhanced** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

Prior to Cisco IOS Release 12.4(24)T, you can configure this command for IP SLAs VoIP RTP operation but operations are unaffected.

In Cisco IOS Release 12.4(24)T and later releases, you cannot configure this command for IP SLAs VoIP RTP operations. If you attempt to configure this command in voip rtp configuration mode, the following message appears.

```
Router(config-ip-sla-voip-rtp)# history enhanced interval 1200 buckets 99
%enhanced-history cannot be set for this probe
```

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

Examples

In the following examples, an Internet Control Message Protocol (ICMP) echo operation is configured with the standard enhanced history characteristics. The example shows the **history enhanced** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 3
 icmp-echo 172.16.1.175
 history enhanced interval 900 buckets 100
!
ip sla schedule 3 start-time now life forever
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 3
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# history enhanced interval 900 buckets 100
Router(config-icmp-ech-params)# end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: 3
    Measure Type: icmp-echo (control enabled)
.
.
.
Statistics Aggregation option:
        Hours of statistics kept: 2
        Enhanced aggregation interval: 900 seconds
        Max number of enhanced interval buckets: 100
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
show ip sla auto summary-statistics	Displays the current operational status and statistics for IP SLAs auto-measure groups.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
show ip sla enhanced-history collection-statistics	Displays data for all collected history buckets for the specified IP SLAs operation, with data for each bucket shown individually.
show ip sla enhanced-history distribution-statistics	Displays enhanced history data for all collected buckets in a summary table.

history filter

To define the type of information kept in the history table for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **history filter** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

history filter {**none** | **all** | **overThreshold** | **failures**}

no history filter {**none** | **all** | **overThreshold** | **failures**}

Syntax Description

none	No history is kept. This is the default.
all	All operations attempted are kept in the history table.
overThreshold	Only packets that are over the threshold are kept in the history table.
failures	Only packets that fail for any reason are kept in the history table.

Command Default

No IP SLAs history is kept for an operation.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **filter-for-history** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.

Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **filter-for-history** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **filter-for-history** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **filter-for-history** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, TCP connect, and UDP echo configuration submodes in IP SLA template parameters configuration mode were added.

Usage Guidelines

Use the **history filter** command to control what gets stored in the history table for an IP SLAs operation. To control how much history gets saved in the history table, use the **history lives-kept**, **history buckets-kept**, and the **samples-of-history-kept** commands.

The **history filter** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

For auto IP SLAs in Cisco IOS IP SLAs Engine 3.0—Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

An IP SLAs operation can collect history and capture statistics. By default, the history for an IP SLAs operation is not collected. When a problem arises where history is useful (for example, a large number of timeouts are occurring), use the **history lives-kept** command to enable history collection.

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

Examples

In the following example, only operation packets that fail are kept in the history table. The example shows the **history filter** command being used in an IPv4 network.

IP SLA auto-Measure Template

```
ip sla auto template type ip icmp-echo
 icmp-echo 172.16.161.21
  history lives-kept 1
  history filter failures
!
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# history filter failures
Router(config-icmp-ech-params)# end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: 1
    Measure Type: icmp-echo
.
.
.
Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: failures
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
history buckets-kept	Sets the number of history buckets that are kept during the lifetime of the IP SLAs operation.
history lives-kept	Sets the number of lives maintained 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 auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the IP SLAs operation.

history hours-of-statistics-kept

To set the number of hours for which statistics are maintained for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **history hours-of-statistics-kept** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

history hours-of-statistics-kept *hours*

no history hours-of-statistics-kept

Syntax Description

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

Command Default

The default is 2 hours.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
ICMP jitter configuration (config-icmp-jtr-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **hours-of-statistics-kept** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.

Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **hours-of-statistics-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **hours-of-statistics-kept** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **hours-of-statistics-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, ICMP jitter, TCP connect, UDP echo, and UDP jitter configuration submodes in IP SLA template parameters configuration mode were added.

Usage Guidelines

When the number of hours exceeds the specified value, the statistics table wraps (that is, the oldest information is replaced by newer information).

For the IP SLAs Internet Control Message Protocol (ICMP) path echo operation, the amount of router memory required to maintain the distribution statistics table is based on multiplying all of the values set by the following four commands:

- **history distributions-of-statistics-kept**
- **hops-of-statistics-kept**
- **paths-of-statistics-kept**
- **history hours-of-statistics-kept**

The general equation used to calculate the memory requirement to maintain the distribution statistics table for an ICMP path echo operation is as follows:
Memory allocation = (160 bytes) * (**history distributions-of-statistics-kept** *size*) * (**hops-of-statistics-kept** *size*) * (**paths-of-statistics-kept** *size*) * (**history hours-of-statistics-kept** *hours*)

Note To avoid significant impact on router memory, careful consideration should be used when configuring the **history distributions-of-statistics-kept**, **hops-of-statistics-kept**, **paths-of-statistics-kept**, and **history hours-of-statistics-kept** commands.

The **history hours-of-statistics-kept** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

For auto IP SLAs in Cisco IOS IP SLAs Engine 3.0—Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

Examples

The following examples shows how to maintain 3 hours of statistics for an ICMP echo operation. The example shows the **history hours-of-statistics-kept** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 2
 icmp-echo 172.16.1.177
 history hours-of-statistics-kept 3
!
ip sla schedule 2 life forever start-time now
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 2
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# history hours-of-statistics-kept 3
Router(config-icmp-ech-params)# end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: 2
    Measure Type: icmp-echo
.
.
.
Statistics Aggregation option:
        Hours of statistics kept: 3
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
history distributions-of-statistics-kept	Sets the number of statistics distributions kept per hop during the lifetime of the IP SLAs operation.
history statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the IP SLAs operation.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.

history lives-kept

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

history lives-kept *lives*

no history lives-kept

Syntax Description

lives	Number of lives maintained in the history table for the operation. If you specify 0 lives, history is not collected for the operation.

Command Default

The default is 0 lives.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Configuration

ICMP echo configuration (config-icmp-ech-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **lives-of-history-kept** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **lives-of-history-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **lives-of-history-kept** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **lives-of-history-kept** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, TCP connect, and UDP echo configuration submodes in IP SLA template parameters configuration mode were added.

Usage Guidelines

The following rules apply to the **history lives-kept** command:

- The number of lives you can specify is dependent on the type of operation you are configuring.
- The default value of 0 lives means that history is not collected for the operation.
- When the number of lives exceeds the specified value, the history table wraps (that is, the oldest information is replaced by newer information).
- When an operation makes a transition from a pending to active state, a life starts. When the life of an operation ends, the operation makes a transition from an active to pending state.

The **history lives-kept** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

To disable history collection, use the **no history lives-kept** command rather than the **history filter none** command. The **no history lives-kept** command disables history collection before an IP SLAs operation is attempted. The **history filter** command checks for history inclusion after the operation attempt is made.

Examples

The following example shows how to maintain the history for five lives of an ICMP echo operation. The example shows the **history lives-kept** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 1
 icmp-echo 172.16.1.176
 history lives-kept 5
!
ip sla schedule 1 life forever start-time now
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# history lives-kept 5
```

```
Router(config-icmp-ech-params)# end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: 1
    Measure Type: icmp-echo
.
.
.
Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 5
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
history buckets-kept	Sets the number of history buckets that are kept during the lifetime of the IP SLAs operation.
history filter	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 auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the IP SLAs operation.

history statistics-distribution-interval

To set the time interval for each statistics distribution kept for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **history statistics-distribution-interval** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

history statistics-distribution-interval *milliseconds*

no history statistics-distribution-interval

Syntax Description

milliseconds	Number of milliseconds (ms) used for each statistics distribution kept. The default is 20.

Command Default

The default interval used for each statistics kept is 20 ms.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
ICMP jitter configuration (config-icmp-jtr-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **statistics-distribution-interval** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.

Release	Modification
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **statistics-distribution-interval** command. The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **statistics-distribution-interval** command. The following configuration modes were added: • Ethernet echo • Ethernet jitter • VCCV
12.4(20)T	The Ethernet echo and Ethernet jitter configuration modes were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **statistics-distribution-interval** command. The Ethernet echo and Ethernet jitter configuration modes were added.
15.1(1)T	This command was modified. The ICMP echo, ICMP jitter, TCP connect, UDP echo, and UDP jitter configuration submodes in IP SLA template parameters configuration mode were added.

Usage Guidelines

In most situations, you do not need to change the time interval for each statistics distribution or number of distributions kept. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network.

To set the number of statistics distributions kept, use the **history statistics-distribution-interval** command.

The **history statistics-distribution-interval** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

Examples

In the following examples, the statistics distribution is set to five and the distribution interval is set to 10 ms for an IP SLAs operation. Consequently, the first distribution will contain statistics from 0 to 9 ms, the second distribution will contain statistics from 10 to 19 ms, the third distribution will contain statistics from 20 to 29 ms, the fourth distribution will contain statistics from 30 to 39 ms, and the fifth distribution will contain statistics from 40 ms to infinity.

The example shows the **history statistics-distribution-interval** command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 1
 icmp-echo 172.16.161.21
 history distributions-of-statistics-kept 5
 history statistics-distribution-interval 10
!
ip sla schedule 1 life forever start-time now
```

IP SLA Template Parameters Configuration

```
Router(config)#ip sla auto template type ip icmp-echo 3
Router(config-tplt-icmp-ech)#parameters
Router(config-icmp-ech-params)#history enhanced interval 900 buckets 100
Router(config-icmp-ech-params)#end
Router# show ip sla auto template type ip udp-echo
R1#show ip sla auto template type ip icmp-echo 5
IP SLAs Auto Template: 5
    Measure Type: icmp-echo
.
.
.
History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 10
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
history distributions-of-statistics-kept	Sets the number of statistics distributions kept per hop during the IP SLAs operation's lifetime.
history hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.

hops-of-statistics-kept

To set the number of hops for which statistics are maintained per path for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **hops-of-statistics-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.

hops-of-statistics-kept *size*

no hops-of-statistics-kept

Syntax Description

size	Number of hops for which statistics are maintained per path. The default is 16.

Defaults

16 hops

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

When the number of hops reaches the size specified, no further hop-based information is stored.

Note This command is supported by the IP SLAs Internet Control Message Protocol (ICMP) path echo operation only.

For the IP SLAs ICMP path echo operation, the amount of router memory required to maintain the distribution statistics table is based on multiplying all of the values set by the following four commands:

- **distributions-of-statistics-kept**

- **hops-of-statistics-kept**
- **paths-of-statistics-kept**
- **hours-of-statistics-kept**

The general equation used to calculate the memory requirement to maintain the distribution statistics table for an ICMP path echo operation is as follows:
Memory allocation = (160 bytes) * (**distributions-of-statistics-kept** *size*) * (**hops-of-statistics-kept** *size*) * (**paths-of-statistics-kept** *size*) * (**hours-of-statistics-kept** *hours*)

Note To avoid significant impact on router memory, careful consideration should be used when configuring the **distributions-of-statistics-kept**, **hops-of-statistics-kept**, **paths-of-statistics-kept**, and **hours-of-statistics-kept** commands.

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 8). 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 **hops-of-statistics-kept** command varies depending on the Cisco IOS release you are running (see Table 8) 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 **hops-of-statistics-kept** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

Table 8 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

The following examples show how to monitor the statistics of IP SLAs ICMP path echo operation 2 for ten hops only. 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 8).

IP SLA Configuration

```
ip sla 2
 path-echo 172.16.1.177
 hops-of-statistics-kept 10
!
ip sla schedule 2 life forever start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 2
 type pathecho protocol ipIcmpEcho 172.16.1.177
 hops-of-statistics-kept 10
```

```
!
ip sla monitor schedule 2 life forever start-time now
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistics distributions kept per hop during the lifetime of the IP SLAs operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained 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.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the IP SLAs operation.

hours-of-statistics-kept

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **hours-of-statistics-kept** command is replaced by the **history hours-of-statistics-kept** command. See the **history hours-of-statistics-kept** command for more information.

To set the number of hours for which statistics are maintained for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **hours-of-statistics-kept** command in the appropriate submode of IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

hours-of-statistics-kept *hours*

no hours-of-statistics-kept

Syntax Description

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

Defaults

2 hours

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **history hours-of-statistics-kept** command.
12.2(33)SRB	This command was replaced by the **history hours-of-statistics-kept** command.
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.

Release	Modification
12.2(33)SB	This command was replaced by the **history hours-of-statistics-kept** command.
12.2(33)SXI	This command was replaced by the **history hours-of-statistics-kept** command.

Usage Guidelines

When the number of hours exceeds the specified value, the statistics table wraps (that is, the oldest information is replaced by newer information).

For the IP SLAs Internet Control Message Protocol (ICMP) path echo operation, the amount of router memory required to maintain the distribution statistics table is based on multiplying all of the values set by the following four commands:

- **distributions-of-statistics-kept**
- **hops-of-statistics-kept**
- **paths-of-statistics-kept**
- **hours-of-statistics-kept**

The general equation used to calculate the memory requirement to maintain the distribution statistics table for an ICMP path echo operation is as follows:
Memory allocation = (160 bytes) * (**distributions-of-statistics-kept** *size*) * (**hops-of-statistics-kept** *size*) * (**paths-of-statistics-kept** *size*) * (**hours-of-statistics-kept** *hours*)

Note To avoid significant impact on router memory, careful consideration should be used when configuring the **distributions-of-statistics-kept**, **hops-of-statistics-kept**, **paths-of-statistics-kept**, and **hours-of-statistics-kept** commands.

Note 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.

Examples

The following example shows how to maintain 3 hours of statistics for IP SLAs ICMP path echo operation 2.

```
ip sla monitor 2
 type pathecho protocol ipIcmpEcho 172.16.1.177
 hours-of-statistics-kept 3
!
ip sla monitor schedule 2 life forever start-time now
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistics distributions kept per hop during the lifetime of the IP SLAs operation.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the IP SLAs operation.

hours-of-statistics-kept (LSP discovery)

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

hours-of-statistics-kept *hours*

no hours-of-statistics-kept

Syntax Description

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

Command Default

2 hours

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

http (IP SLA)

To configure a Cisco IOS IP Service Level Agreements (SLAs) HTTP operation, use the **http** command in IP SLA configuration mode.

http {**get** | **raw**} *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]

Syntax Description

get	Specifies an HTTP GET operation.
raw	Specifies an HTTP RAW operation.
url	URL of destination HTTP server.
name-server *ip-address*	(Optional) Specifies the destination IP address of a Domain Name System (DNS) Server.
version *version-number*	(Optional) Specifies the version number.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
cache {**enable** | **disable**}	(Optional) Enables or disables download of a cached HTTP page.
proxy *proxy-url*	(Optional) Specifies proxy information or URL.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type http operation** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type http operation** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type http operation** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type http operation** command.

Usage Guidelines

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

Examples

In the following example, IP SLAs HTTP operation 6 is configured as an HTTP RAW operation. The destination URL is http://www.cisco.com.

```
ip sla 6
 http raw http://www.cisco.com
 http-raw-request
 GET /index.html HTTP/1.0\r\n
 \r\n
!
ip sla schedule 6 start-time now
```

Related Commands

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

http-raw-request

To explicitly specify the options for a GET request for a Cisco IOS IP Service Level Agreements (SLAs) Hypertext Transfer Protocol (HTTP) operation, use the **http-raw-request** command in the appropriate submode of IP SLA configuration or IP SLA monitor configuration mode.

http-raw-request

Syntax Description

This command has no arguments or keywords.

Defaults

No options are specified for a GET request.

Command Modes

IP SLA Configuration

HTTP configuration (config-ip-sla-http)

IP SLA Monitor Configuration

HTTP configuration (config-sla-monitor-http)

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
12.0(5)T	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

Use the **http-raw-request** command to explicitly specify the content of an HTTP request. Use HTTP version 1.0 commands after entering the **http-raw-request** command.

IP SLAs will specify the content of an HTTP request if you use the **type http operation get** command. IP SLAs will send the HTTP request, receive the reply, and report round-trip time (RTT) statistics (including the size of the page returned).

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 9). 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 **http-raw-request** command varies depending on the Cisco IOS release you are running (see Table 9) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the HTTP operation type is configured, you would enter the **http-raw-request** command in HTTP configuration mode (config-sla-monitor-http) within IP SLA monitor configuration mode.

Table 9 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, IP SLAs operation 6 is created and configured as an HTTP operation. The HTTP **GET** command is explicitly specified. 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 9).

IP SLA Configuration

```
ip sla 6
 http raw http://www.cisco.com
 http-raw-request
 GET /index.html HTTP/1.0\r\n
 \r\n
!
ip sla schedule 6 start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 6
 type http operation raw url http://www.cisco.com
 http-raw-request
 GET /index.html HTTP/1.0\r\n
 \r\n
!
ip sla monitor schedule 6 start-time now
```

Related Commands

Command	Description
http (IP SLA)	Configures an HTTP IP SLAs operation in IP SLA 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.
type http operation	Configures an HTTP IP SLAs operation in IP SLA monitor configuration mode.

icmp-echo

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **icmp-echo** command in IP SLA configuration mode.

icmp-echo {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-interface *interface-name*	(Optional) Specifies the source interface for the operation.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type echo protocol ipIcmpEcho** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type echo protocol ipIcmpEcho** command.
12.2(33)SRC	Support for IPv6 addresses was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type echo protocol ipIcmpEcho** command. Support for IPv6 addresses was added.
12.4(20)T	Support for IPv6 addresses was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type echo protocol ipIcmpEcho** command. The keyword source-interface is not supported.

Usage Guidelines

The default request packet data size for an ICMP echo operation is 28 bytes. Use the **request-data-size** command to modify this value. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.

You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or ICMP echo) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla** global configuration command) and then reconfigure the operation with the new operation type.

IP SLAs ICMP echo operations support both IPv4 and IPv6 addresses.

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the ICMP protocol and the destination IPv4 address 172.16.1.175:

```
ip sla 10
 icmp-echo 172.16.1.175
!
ip sla schedule 10 start-time now
```

In the following example, IP SLAs operation 11 is created and configured as an echo operation using the ICMP protocol and the destination IPv6 address 2001:DB8:100::1:

```
ip sla 11
 icmp-echo 2001:DB8:100::1
!
ip sla schedule 11 start-time now
```

Related Commands

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

icmp-jitter

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) jitter operation, use the **icmp-jitter** command in IP SLA configuration mode.

icmp-jitter {*destination-ip-address* | *destination-hostname*} [**interval** *milliseconds*] [**num-packets** *packet-number*] [**source-ip** {*ip-address* | *hostname*}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
interval *milliseconds*	(Optional) Specifies the time interval between packets (in milliseconds). The default value is 20 ms.
num-packets *packet-number*	(Optional) Specifies the number of packets to be sent in each operation. The default value is 10 packets per operation.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.

Command Default

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.

Usage Guidelines

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

Examples

The following example shows how to configure an IP SLAs ICMP jitter operation:

```
ip sla 1
 icmp-jitter 172.18.1.129 interval 40 num-packets 100 source-ip 10.1.2.34
 frequency 50
!
ip sla reaction-configuration 1 react jitterAvg threshold-value 5 2 action-type trap
threshold-type immediate
!
ip sla schedule 1 start-time now life forever
```

Related Commands

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

interval (LSP discovery)

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

interval *milliseconds*

no interval

Syntax Description

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

Command Default

0 milliseconds

Command Modes

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

Command History

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

Usage Guidelines

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

Examples

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

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
```

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

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

interval (params)

To specify the interval between packets for a jitter operation in an auto IP Service Level Agreements (SLAs) operation template, use the **interval** command in the appropriate submode of IP SLA template parameters configuration mode. To return to the default, use the **no** form of this command.

interval *milliseconds*

no interval

Syntax Description

milliseconds	Interval between packets in milliseconds (ms). Range is from 4 to 60000. Default is 20.

Command Default

The default interval between packets is 20 ms.

Command Modes

IP SLA Template Parameters Configuration

ICMP jitter configuration (config-icmp-jtr-params)
UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the interval between packets sent during a jitter operation from the default (20 ms) to the specified interval.

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

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

Examples

The following example shows how to configure an auto IP SLAs operation template for an ICMP jitter operation with an interval of 30 ms between packets:

```
Router(config)#ip sla auto template type ip icmp-jitter 1
Router(config-tplt-icmp-jtr)#parameters
Router(config-icmp-jtr-params)#interval 30
Router(config-icmp-jtr-params)#end
Router# show ip sla auto template type ip icmp-jitter
IP SLAs Auto Template: 1
    Measure Type: icmp-jitter
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
```

```
    Number of Packets: 10   Inter packet interval: 30
    Timeout: 5000           Threshold: 5000
Statistics Aggregation option:
    Hours of statistics kept: 2
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

Related Commands

Command	Description
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
show ip sla auto template	Displays configuration including default values of an auto IP SLAs operation template.

ip-address (endpoint list)

To specify destination IP addresses for routing devices or Cisco IOS IP Service Level Agreements (SLAs) Responders in Cisco devices and add them to an auto IP SLAs endpoint list, use the **ip-address** command in IP SLA endpoint-list configuration mode. To remove some or all IP addresses from the template, use the **no** form of this command.

ip-address *address* [**-***address* | **,...,***address*] **port** *port*

no ip-address *address* [*address*-*address* | **,...,***address*] **port** *port*

Syntax Description

address	IPv4 address of destination routing device or destination IP SLAs responder.
-*address*	(Optional) Last IP address in a range of contiguous IP addresses. The hyphen (-) is required.
,...,*address*	(Optional) List of up to five individual IP addresses separated by commas (**,**). Do not type the ellipses (...).
port *port*	Specifies port number of destination routing device or destination IP SLAs responder. Range is from 1 to 65535.

Command Default

The auto IP SLAs endpoint list is empty.

Command Modes

IP SLA endpoint-list configuration (config-epl)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command adds IP addresses to the auto IP SLAs endpoint list being configured.

Destination IP addresses can either be manually configured by using this command or automatically discovered by using the **discover** command. If you use this command to configure an auto IP SLAs endpoint list, you cannot use the **discover** command to discover IP addresses for this endpoint list.

You cannot combine a list of individual IP addresses (*address***,***address*) and a range of IP addresses (*address*-*address*) in a single command.

The maximum number of IP addresses allowed in a list of individual addresses (*address***,***address*) per command is five.

To remove one or more IP addresses without reconfiguring the entire template, use the **no** form of this command. You can delete a range of IP addresses or a single IP addresses per command.

Modifications to auto IP SLAs endpoint lists, such as adding or removing IP addresses, take effect in the next schedule cycle.

Use the **destination** command in IP SLA auto-measure group configuration mode to specify an endpoint list for an IP SLAs auto-measure group.

Examples

The following example shows how to configure an IP SLAs endpoint list using this command:

```
Router(config)#ip sla auto endpoint-list type ip test
Router(config-epl)#ip-address 10.1.1.1-13 port 5000
Router(config-epl)#no ip-address 10.1.1.3-4 port 5000
Router(config-epl)#no ip-address 10.1.1.8 port 5000
Router(config-epl)#no ip-address 10.1.1.12 port 5000
Router(config-epl)#exit
Router#
```

The following output from the **show ip sla auto endpoint** command shows the results of the preceding configuration:

```
Router# show ip sla auto endpoint-list
Endpoint-list Name: test
    Description:
    ip-address 10.1.1.1-2 port 5000
    ip-address 10.1.1.5-7 port 5000
    ip-address 10.1.1.9-11 port 5000
    ip-address 10.1.1.13 port 5000
```

Related Commands

Command	Description
discover (epl)	Enters IP SLA endpoint-list auto-discovery configuration mode for building a list of destination IP addresses.
show ip sla auto endpoint-list	Displays configuration including default values of auto IP SLAs endpoint lists.

ip sla

To begin configuring a Cisco IOS IP Service Level Agreements (SLAs) operation and enter IP SLA configuration mode, use the **ip sla** 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.

ip sla *operation-number*

no ip sla *operation-number*

Syntax Description

operation-number	Operation number used for the identification of the IP SLAs operation you want to configure.

Defaults

No IP SLAs operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

The **ip sla** command is used to begin configuration for an IP SLAs operation. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, the router will enter IP SLA configuration mode.

The **ip sla** command is supported in IPv4 networks. This command can also be used when configuring an IP SLAs operation that supports IPv6 addresses.

IP SLAs allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

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

To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla**) and then reconfigure the operation with the new operation type.

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 ip sla** command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show ip sla configuration** command in user EXEC or privileged EXEC mode.

Examples

In the following example, operation 99 is configured as a UDP jitter operation in an IPv4 network and scheduled to start running in 5 hours. The example shows the **ip sla** command being used in an IPv4 network.

```
ip sla 99
 udp-jitter 172.29.139.134 dest-port 5000 num-packets 20
!
ip sla schedule 99 life 300 start-time after 00:05:00
```

Note If operation 99 already exists and has not been scheduled, the command line interface will enter IP SLA configuration mode for operation 99. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
ip sla group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
ip sla reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
ip sla 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 reaction-configuration** command.
ip sla schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

ip sla auto discovery

To enable auto discovery in Cisco IOS IP Service Level Agreements (SLAs) Engine 3.0, use the **ip sla auto discovery** command in global configuration mode. To disable auto discovery, use the **no** form of this command.

ip sla auto discovery

no ip sla auto discovery

Syntax Description

This command has no arguments or keywords.

Command Default

Auto discovery is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables the source for IP SLAs operations to auto-discover Cisco IP SLAs Responder endpoints.

Examples

The following example shows how to configure the **ip sla auto discovery** command:

```
Router>show ip sla auto discovery
IP SLAs auto-discovery status: Disabled

The following Endpoint-list are configured to auto-discovery:

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip sla auto discovery
Router(config)#exit
Router#
Router# show ip sla auto discovery
IP SLAs auto-discovery status: Enabled

The following Endpoint-list are configured to auto-discovery:
.
.
.
```

Related Commands

Command	Description
show ip sla auto discovery	Displays the status of IP SLAs auto discovery and the configuration of auto IP SLAs endpoint lists configured using auto discovery.

ip sla auto endpoint-list

To enter IP SLA endpoint-list configuration mode and begin configuring an auto IP Service Level Agreements (SLAs) endpoint list, use the **ip sla auto endpoint-list** command in global configuration mode. To remove an endpoint list, use the **no** form of this command.

ip sla auto endpoint-list type ip *template-name*

no ip sla auto endpoint-list *template-name*

Syntax Description

type ip	Specifies that the operation type is Internet Protocol (IP).
template-name	Unique identifier of the endpoint list. Length of string is 1 to 64 ASCII characters.

Command Default

No auto IP SLAs endpoint list is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command assigns a name to an auto IP SLAs endpoint list and enters IP SLA endpoint-list configuration mode on the router.

Use the commands in IP SLA endpoint-list configuration mode to configure a template of destination IP addresses of routing devices or Cisco IOS IP SLAs Responders in Cisco devices to be referenced by one or more IP SLAs auto-measure groups. Destination addresses can be either manually configured by using the **ip-address** command or automatically discovered using the **discover** command.

Each auto IP SLAs endpoint list can be referenced by one or more IP SLAs auto-measure groups. Use the **destination** command in IP SLA auto-measure group configuration mode to specify an endpoint list for an IP SLAs auto-measure group.

Examples

The following example shows how to configure two auto IP SLAs endpoint lists of endpoints, one by manually configuring destination IP addresses and one using auto discovery:

```
Router(config)# ip sla auto endpoint-list type ip man1
Router(config-epl)# ip-address 10.1.1.1-10.1.1.12 port 23
Router(config-epl)# ip-address 10.1.1.15,10.1.1.23 port 23
Router(config-epl)# no ip-address 10.1.1.8,10.1.1.10 port 23
Router(config-epl)# description testing manual build
Router(config-epl)# exit
Router(config)#
Router(config)#ip sla auto discover
Router(config)#ip sla auto endpoint-list type ip autolist
Router(config-epl)#discover port 5000
```

```
Router(config-epl)#access-list 3
Router(config-epl)#exit
Router#
Router# show ip sla auto endpoint-list
Endpoint-list Name: man1
    Description: testing manual build
    ip-address 10.1.1.1-7 port 23
    ip-address 10.1.1.9,10.1.1.15,10.1.1.23 port 23
Endpoint-list Name: autolist
    Description:
    Auto Discover Parameters
        Destination Port: 5000
        Access-list: 3
        Ageout: 3600    Measurement-retry: 3

    1 endpoints are discovered for autolist
```

Related Commands

Command	Description
destination (am-group)	Specifies an endpoint list for an IP SLAs auto-measure group.
discover (epl)	Enters IP SLA endpoint-list auto-discovery configuration mode for building an IP SLAs endpoint list.
ip-address (epl)	Configures and adds endpoints to an IP SLAs endpoint list.
show ip sla auto endpoint-list	Displays configuration including default values of auto IP SLAs endpoint lists.

ip sla auto group

To enter IP SLA auto-measure group configuration mode and begin configuring a Cisco IOS IP Service Level Agreements (SLAs) auto-measure group, use the **ip sla auto group** command in global configuration mode. To remove the auto-measure group configuration, use the **no** form of this command.

ip sla auto group type ip *group-name*

no ip sla auto group *group-name*

Syntax Description

type ip	Specifies that the operation type for the group is Internet Protocol (IP).
group-name	Identifier of the group. String of 1 to 64 ASCII characters.

Command Default

No IP SLAs auto-measure group is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command assigns a name to an IP SLAs auto-measure group and enters IP SLA auto-measure group configuration mode.

Use the commands in IP SLA auto-measure group configuration mode to specify an auto IP SLAs operation template, endpoint list, and scheduler for the group.

Examples

The following example shows how to configure an IP SLAs auto-measure group:

```
Router(config)#ip sla auto group type ip 1
Router(config-am-grp)#destination 1
Router(config-am-grp)#schedule 1
Router(config-am-grp)#end
Router#
Router# show ip sla auto group
Group Name: 1
    Description:
    Activation Trigger: Immediate
    Destination: 1
    Schedule: 1

IP SLAs Auto Template: default
    Measure Type: icmp-jitter
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
```

```
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None

IP SLAs auto-generated operations of group 1
    no operation created
```

Related Commands

Command	Description
show ip sla auto group	Displays configuration including default values of IP SLAs auto-measure groups.

ip sla auto schedule

To enter IP SLA auto-measure schedule configuration mode and begin configuring an auto IP Service Level Agreements (SLAs) scheduler, use the **ip sla auto schedule** command in global configuration mode. To remove the configuration and stop all operations controlled by this scheduler, use the **no** form of this command.

ip sla auto schedule *schedule-id*

no ip sla auto schedule *schedule-id*

Syntax Description

schedule-id	Unique identifier of scheduler. Range is 1 to 64 alphanumeric characters.

Command Default

No auto IP SLAs scheduler is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command assigns a unique identifier to an auto IP SLAs scheduler and enters IP SLA auto-measure schedule configuration mode on the router.

Use the commands in IP SLA auto-measure schedule configuration mode to modify the default configuration of an auto IP SLAs scheduler.

Each auto IP SLAs scheduler can be referenced by one or more IP SLAs auto-measure groups. Use the **schedule** command in IP SLA auto-measure group configuration mode to specify a scheduler for an IP SLAs auto-measure group.

Examples

The following example shows how to create the default configuration for an auto IP SLAs scheduler:

```
Router(config)#ip sla auto schedule 2
Router(config-am-schedule)#end
Router#
Router# show ip sla auto schedule 2
Group sched-id: 2
    Probe Interval (ms) : 1000
    Group operation frequency (sec): 60
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: Pending trigger
    Life (sec): 3600
    Entry Ageout (sec): never
```

Related Commands

Command	Description
schedule	Specifies an auto IP SLAs scheduler for an IP SLAs auto-measure group.
show ip sla auto schedule	Displays configuration including default values of auto IP SLAs schedulers.

ip sla auto template

To enter IP SLA template configuration mode and begin configuring an auto IP Service Level Agreements (SLAs) operation template, use the **ip sla auto template** command in global configuration mode. To remove the operation template, use the **no** form of this command.

ip sla auto template type ip *operation template-name*

no ip sla auto template type ip *operation template-name*

Syntax Description

type ip	Specifies that the operation type is Internet Protocol (IP).
operation	Type of IP operation for this template. Use one of the following keywords: • **icmp-echo**—Internet Control Message Protocol (ICMP) echo operation • **icmp-jitter—**Internet Control Message Protocol (ICMP) jitter operation • **tcp-connect—**Transmission Control Protocol (TCP) connection operation • **udp-echo—**User Datagram Protocol (UDP) echo operation • **udp-jitter—**User Datagram Protocol (UDP) jitter operation
template-name	Identifier of template. String of 1 to 64 alphanumeric characters.

Command Default

No IP SLAs operation template is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command assigns a name and operation to an auto IP SLAs operation template and enters a submode of the IP SLA template configuration mode based on the specified *operation* argument, such as IP SLA template icmp-echo configuration submode (config-tplt-icmp-ech).

Use the commands in IP SLA template configuration submode to modify the default configuration of an auto IP SLAs operation template.

Each auto IP SLAs operation template can be referenced by one or more IP SLAs auto-measure groups. Use the **template** command in IP SLA auto-measure group configuration mode to specify an operation template for an IP SLAs auto-measure group.

Examples

The following example shows how to create a default configuration for an auto IP SLAs operation template for ICMP echo:

```
Router(config)# ip sla auto template type ip icmp-echo
```

```
Router(config-tplt-icmp-ech)#end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: basic_icmp_echo
    Measure Type: icmp-echo
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 28   Verify Data: false
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
template	Specifies an auto IP SLAs operation template for an IP SLAs auto-measure group.
show ip sla auto template	Display configuration including default values of auto IP SLAs operation templates.

ip sla enable reaction-alerts

To enable Cisco IP Service Level Agreements (SLAs) notifications to be sent to all registered applications, use the **ip sla enable reaction-alerts** command in global configuration mode. To disable IP SLAs notifications, use the **no** form of this command.

ip sla enable reaction-alerts

no ip sla enable reaction-alerts

Syntax Description

This command has no arguments or keywords.

Command Default

IP SLAs notifications are not sent to registered applications.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The only applications that can register are Cisco IOS processes running on the router. Proactive threshold monitoring parameters for a Cisco IOS IP SLAs operation can be configured that will generate notifications when a threshold is crossed.

Examples

The following example shows how to enable IP SLAs notifications to be sent to all registered applications:

```
Router(config)# ip sla enable reaction-alerts
```

Related Commands

Command	Description
debug ip sla error	Enables debugging output of IP SLAs operation run-time errors.
debug ip sla trace	Traces the execution of IP SLAs operations.
ip sla reaction-configuration	Configures proactive threshold monitoring parameters for a Cisco IOS IP SLAs operation.
show ip sla application	Displays global information about Cisco IOS IP SLAs.
show ip sla event-publisher	Displays a list of clients registered to receive IP SLAs notifications.

ip sla ethernet-monitor

To begin configuring a Cisco IOS IP Service Level Agreements (SLAs) auto Ethernet operation and enter IP SLA Ethernet monitor configuration mode, use the **ip sla ethernet-monitor** command in global configuration mode. To remove all configuration information for an auto Ethernet operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

ip sla ethernet-monitor *operation-number*

no ip sla ethernet-monitor *operation-number*

Syntax Description

operation-number	Operation number used for the identification of the IP SLAs operation you want to configure.

Command Default

No IP SLAs operation is configured.

Command Modes

Global configuration (config)

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.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

The **ip sla ethernet-monitor** command is used to begin configuration for an IP SLAs auto Ethernet operation. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, the router will enter IP SLA Ethernet monitor configuration mode.

After you configure an auto Ethernet operation, you must schedule the operation. To schedule an auto Ethernet operation, use the **ip sla ethernet-monitor schedule** command in global configuration mode. You can also optionally set reaction configuration for the operation (see the **ip sla ethernet-monitor reaction-configuration** command).

To display the current configuration settings of an auto Ethernet operation, use the **show ip sla ethernet-monitor configuration** command in user EXEC or privileged EXEC mode.

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using an IP SLAs auto Ethernet operation. In this example, operation 10 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance endpoints in the domain named testdomain and VLAN identification number 34. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss events occur, a Simple Network Management Protocol (SNMP) trap notification should be sent. The schedule period for operation 10 is 60 seconds, and the operation is scheduled to start immediately.

```
ip sla ethernet-monitor 10
 type echo domain testdomain vlan 34
!
ip sla ethernet-monitor reaction-configuration 10 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

Related Commands

Command	Description
ip sla ethernet-monitor reaction-configuration	Configures the proactive threshold monitoring parameters for an IP SLAs auto Ethernet operation.
ip sla ethernet-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.
show ip sla ethernet-monitor configuration	Displays configuration settings for IP SLAs auto Ethernet operations.

ip sla ethernet-monitor reaction-configuration

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

ip sla ethernet-monitor reaction-configuration *operation-number* [**react** *monitored-element* [**action-type** {**none** | **trapOnly**}] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]

no ip sla ethernet-monitor reaction-configuration *operation-number* [**react** *monitored-element*]

Syntax Description

operation-number	Number of the IP SLAs operation for which reactions are to be configured.
react *monitored-element*	(Optional) Specifies the element to be monitored for threshold violations. Keyword options for the monitored-element argument are as follows: • **connectionLoss**—Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. • **jitterAvg**—Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg**—Specifies that a reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg**—Specifies that a reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold. • **maxOfNegativeDS**—Specifies that a reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD**—Specifies that a reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated. • **maxOfPositiveDS**—Specifies that a reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD**—Specifies that a reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated.

react *monitored-element* (continued)	• **packetLateArrival**—Specifies that a reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLossDS**—Specifies that a reaction should occur if the one-way destination-to-source packet loss value violates the upper threshold or lower threshold. • **packetLossSD**—Specifies that a reaction should occur if the one-way source-to-destination packet loss value violates the upper threshold or lower threshold. • **packetMIA**—Specifies that a reaction should occur if the one-way number of missing packets violates the upper threshold or lower threshold. • **packetOutOfSequence**—Specifies that a reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt**—Specifies that a reaction should occur if the round-trip time violates the upper threshold or lower threshold. • **timeout**—Specifies that a reaction should occur if there is a one-way timeout for the monitored operation.
action-type none	(Optional) Specifies that no action is taken when threshold events occur. The **none** keyword is the default value. **Note** If the **threshold-type never** keywords are configured, the **action-type** keyword is disabled.
action-type trapOnly	(Optional) Specifies that a Simple Network Management Protocol (SNMP) trap notification should be sent when threshold violation events occur. **Note** If the **threshold-type never** keywords are configured, the **action-type** keyword is disabled.
threshold-type average [*number-of-measurements*]	(Optional) Specifies that when the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, the action defined by the **action-type** keyword should be performed. 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. In this case, the average exceeds the upper threshold. The default number of 5 averaged measurements can be changed using the *number-of-measurements* argument. The valid range is from 1 to 16. This syntax is not available if the **connectionLoss** or **timeout** keyword is specified as the monitored element, because upper and lower thresholds do not apply to these options.
threshold-type consecutive [*occurrences*]	(Optional) Specifies that when a threshold violation for the monitored element is met consecutively for a specified number of times, the action defined by the **action-type** keyword should be performed. The default number of 5 consecutive occurrences can be changed using the *occurrences* argument. The valid range is from 1 to 16.

threshold-type immediate	(Optional) Specifies that when a threshold violation for the monitored element is met, the action defined by the **action-type** keyword should be performed immediately.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type.
threshold-type xofy [*x-value y-value*]	(Optional) Specifies that when a threshold violation for the monitored element is met x number of times within the last y number of measurements ("x of y"), action defined by the **action-type** keyword should be performed. The default is 5 for both the x and y values (**xofy 5 5**). The valid range for each value is from 1 to 16.
threshold-value [*upper-threshold lower-threshold*]	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See Table 10 in the "Usage Guidelines" section for a list of the default values.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration (config)

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 can configure the **ip sla ethernet-monitor reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements (for example, configuring thresholds for round-trip time and destination-to-source packet loss) for the same operation. However, disabling of individual monitored elements is not supported. In other words, the **no ip sla ethernet-monitor reaction-configuration** command will disable all proactive threshold monitoring configuration for the specified IP SLAs operation.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **ip sla 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 auto Ethernet operation, use the **show ip sla ethernet-monitor configuration** command.

Table 10 lists the default upper and lower thresholds for specific monitored elements.

Table 10 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms
jitterSDAvg	100 ms	100 ms
maxOfNegativeDS	10000 ms	10000 ms
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
packetLateArrival	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rtt	5000 ms	3000 ms

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using an IP SLAs auto Ethernet operation. In this example, operation 10 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance endpoints in the domain named testdomain and VLAN identification number 34. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss events occur, an SNMP trap notification should be sent. The schedule period for operation 10 is 60 seconds, and the operation is scheduled to start immediately.

```
Router(config)# ip sla ethernet-monitor 10
Router(config-ip-sla-ethernet-monitor)# type echo domain testdomain vlan 34
!
Router(config)# ip sla ethernet-monitor reaction-configuration 10 react connectionLoss
threshold-type consecutive 3 action-type trapOnly
!
Router(config)# ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

Related Commands

Command	Description
ip sla ethernet-monitor	Begins configuration for an IP SLAs auto Ethernet operation and enters Ethernet monitor configuration mode.
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla ethernet-monitor configuration	Displays configuration settings for IP SLAs auto Ethernet operations.
snmp-server enable traps rtr	Enables the sending of IP SLAs SNMP trap notifications.

ip sla ethernet-monitor schedule

To configure the scheduling parameters for an IP Service Level Agreements (SLAs) auto Ethernet operation, use the **ip sla ethernet-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.

ip sla ethernet-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 ip sla ethernet-monitor schedule *operation-number*

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

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

After you schedule an IP SLAs auto Ethernet operation with the **ip sla ethernet-monitor schedule** command, you should not change the configuration of the operation until the operation has finished collecting information. To change the configuration of the operation, use the **no ip sla ethernet-monitor schedule** *operation-number* command in global configuration mode and then enter the new configuration information.

To display the current configuration settings of an IP SLAs auto Ethernet operation, use the **show ip sla ethernet-monitor configuration** command in user EXEC or privileged EXEC mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using an IP SLAs auto Ethernet operation. In this example, operation 10 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance endpoints in the domain named testdomain and VLAN identification number 34. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss events occur, a Simple Network Management Protocol (SNMP) trap notification should be sent. The schedule period for operation 10 is 60 seconds, and the operation is scheduled to start immediately.

```
ip sla ethernet-monitor 10
 type echo domain testdomain vlan 34
!
ip sla ethernet-monitor reaction-configuration 10 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

Related Commands

Command	Description
ip sla ethernet-monitor	Begins configuration for an IP SLAs auto Ethernet operation and enters Ethernet monitor configuration mode.
show ip sla ethernet-monitor configuration	Displays configuration settings for IP SLAs auto Ethernet operations.

ip sla group schedule

To perform multioperation scheduling for Cisco IOS IP Service Level Agreements (SLAs) operations, use the **ip sla group schedule** command in global configuration mode. To cause all the IP SLAs operations belonging to a multioperation schedule to become inactive, use the **no** form of this command.

ip sla group schedule *group-id* {*operation-ids* | **add** *operation-ids* | **delete** *operation-ids* | **reschedule**} **schedule-period** *seconds* [**ageout** *seconds*] [**frequency** [*seconds* | **range** *random-frequency-range*]] [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}]

no ip sla group schedule *group-id*

Syntax Description

group-id	Identification number for the group of IP SLAs operation to be scheduled. The range is from 0 to 65535.
operation-ids	List of one or more identification (ID) numbers of the IP SLAs operations to be included in a new multioperation schedule. The length of this argument is up to 125 characters. 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: • 2, 3, 4, 9, 20 • 10-20, 30-35, 60-70 • 2, 3, 4, 90-100, 105-115 In Cisco IOS Release 15.1(1)T and later releases: A single operation ID is a valid option for this argument.
add *operation-ids*	Specifies the ID numbers of one or more IP SLAs operations to be added to an existing multioperation schedule.
delete *operation-ids*	Specifies the ID numbers of one or more IP SLAs operations to be removed from an existing multioperation schedule.
reschedule	Recalculates the start time for each IP SLAs operation within the multioperation schedule based on the number of operations and the schedule period. Use this keyword after an operation has been added to or removed from an existing multioperation schedule.
schedule-period *seconds*	Specifies the amount of time (in seconds) for which the group of IP SLAs operations is scheduled. The range is from 1 to 604800.
ageout *seconds*	(Optional) Specifies the number of seconds to keep the IP SLAs operations in memory when they are not actively collecting information. The default is 0 (never ages out).
frequency *seconds*	(Optional) Specifies the number of seconds after which each IP SLAs operation is restarted. The frequency of all operations belonging to the multioperation schedule is overridden and set to the specified frequency. The range if from 1 to 604800. **Note** The default frequency is the value specified for the schedule period.

frequency range *random-frequency-range*	(Optional) Enables the random scheduler option. See the "Usage Guidelines" section for more information. The random scheduler option is disabled by default. The frequencies at which the IP SLAs operations within the multioperation schedule will restart are chosen randomly within the specified frequency range (in seconds). Separate the lower and upper values of the frequency range with a hyphen (for example, 80-100).
life forever	(Optional) Schedules the IP SLAs operations to run indefinitely.
life *seconds*	(Optional) Specifies the number of seconds the IP SLAs operations will actively collect information. The default is 3600 (one hour).
start-time	(Optional) Indicates the time at which the group of IP SLAs operations will start 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**.
*hh***:***mm*[**:***ss*]	(Optional) Specifies an absolute start time for the multioperation schedule 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 *month* and *day*.
month	(Optional) Specifies the name of the month in which to start the multioperation schedule. If month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Specifies the number of the day (in the range 1 to 31) on which to start the multioperation schedule. If a day is not specified, the current day is used. Use of this argument requires that a month be specified.
pending	(Optional) Indicates that no information is being collected. This is the default value.
now	(Optional) Indicates that the multioperation schedule should start immediately.
after *hh***:***mm***:***ss*	(Optional) Indicates that the multioperation schedule should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.

Defaults

The multioperation schedule is placed in a **pending** state (that is, the group of IP SLAs operations are enabled but are not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor group schedule** command.
12.4(6)T	The following arguments and keywords were added: • **add** *operation-ids* • **delete** *operation-ids* • **reschedule**
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr group schedule** command. The **range** keyword and *random-frequency-range* argument were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor group schedule** command. The **range** keyword and *random-frequency-range* argument were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor group schedule** command. The **range** keyword and *random-frequency-range* argument were added.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.
15.1(1)T	This command was modified. Support for scheduling a single operation was added.

Usage Guidelines

Though the IP SLAs multioperation scheduling functionality helps in scheduling thousands of operations, you should be cautious when specifying the number of operations, the schedule period, and the frequency to avoid any significant CPU impact.

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:

ip sla group schedule 2 1-780 schedule-period 60 start-time 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 multioperation 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.

On a Cisco 2600 router, the maximum recommended value of operations per second is 6 or 7 (approximately 350 to 400 operations per minute). Exceeding this value of 6 or 7 operations per second could cause major performance (CPU) impact. Note that the maximum recommended value of operations per second varies from platform to platform.

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:

ip sla 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.

IP SLAs Random Scheduler

The IP SLAs random scheduler option provides the capability to schedule multiple IP SLAs operations to begin at random intervals over a specified duration of time. The random scheduler option is disabled by default. To enable the random scheduler option, you must configure the **frequency range** *random-frequency-range* keywords and argument. The operations within the multioperation schedule restart at uniformly distributed random frequencies within the specified frequency range. The following guidelines apply for setting the frequency range:

- The starting value of the frequency range should be greater than the timeout values of all the operations in the multioperation schedule.
- The starting value of the frequency range should be greater than the schedule period (amount of time for which the group of operations is scheduled). This guideline ensures that the same operation does not get scheduled more than once within the schedule period.

The following guidelines apply if the random scheduler option is enabled:

- The individual operations in a multioperation schedule will be uniformly distributed to begin at random intervals over the schedule period.
- The operations within the multioperation schedule restart at uniformly distributed random frequencies within the specified frequency range.
- The minimum time interval between the start of each operation in a multioperation schedule is 100 milliseconds (0.1 seconds). If the random scheduler option is disabled, the minimum time interval is 1 second.
- Only one operation can be scheduled to begin at any given time. If the random scheduler option is disabled, multiple operations can begin at the same time.
- The first operation will always begin at 0 milliseconds of the schedule period.
- The order in which each operation in a multioperation schedule begins is random.

Adding or Deleting IP SLAs Operations

The following guidelines apply when an IP SLAs operation is added to or deleted from an existing multioperation schedule:

- If an operation is added that already belongs to the multioperation schedule, no action is taken.

- If two or more operations are added after the multioperation schedule has started, then the start times of the newly added operations will be uniformly distributed based on a time interval that was calculated prior to the addition of the new operations. If two or more operations are added before the multioperation schedule has started, then the time interval is recalculated based on both the existing and newly added operations.
- If an operation is added to a multioperation schedule in which the random scheduler option is enabled, then the start time and frequency of the newly added operation will be randomly chosen within the specified parameters.
- If an operation is added to a multioperation schedule in which the existing operations have aged out or the lifetimes of the existing operations have ended, the newly added operation will start and remain active for the amount of time specified by the multioperation schedule.
- If an active operation is deleted, then the operation will stop collecting information and become inactive.
- If the **ip sla group schedule** *group-id* **reschedule** command is entered after an operation is added or deleted, the time interval between the start times of the operations is recalculated based on the new number of operations belonging to the multioperation schedule.

Before Cisco IOS Release 15.1(1)T, this command could not be used to schedule a single operation because the only valid options for the *operation-ids* argument were a list (id,id,id) of IDs, a range (id-id) of IDs, or a combination of lists and ranges. If you attempted to use this command to schedule a single operation, the following messages were displayed:

```
Router(config)# sla group schedule 1 1 schedule-period 5 start-time now
%Group Scheduler: probe list wrong syntax
%Group schedule string of probe ID's incorrect
Router(config)#
```

In Cisco IOS Release 15.1(1)T and later releases, a single operation ID is a valid option for the *operation-ids* argument.

Examples

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 (identified as group 1) using multioperation scheduling. In this example, the operations are scheduled to begin at equal intervals over a schedule period of 20 seconds. The first operation (or set of operations) is scheduled to start immediately. Since the frequency is not specified, it is set to the value of the schedule period (20 seconds) by default.

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

The following example shows how to schedule IP SLAs operations 1 to 3 (identified as group 2) using the random scheduler option. In this example, the operations are scheduled to begin at random intervals over a schedule period of 50 seconds. The first operation is scheduled to start immediately. The frequency at which each operation will restart will be chosen randomly within the range of 80 to 100 seconds.

```
ip sla group schedule 2 1-3 schedule-period 50 frequency range 80-100 start-time now
```

Related Commands

Command	Description
ip sla schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla configuration	Displays the configuration details of the IP SLAs operation.
show ip sla group schedule	Displays the group scheduling details of the IP SLAs operations.

ip sla key-chain

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

ip sla key-chain *name*

no ip sla key-chain

Syntax Description

name	Name of MD5 key chain.

Defaults

Control message authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor key-chain** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr key-chain** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor key-chain** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor key-chain** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

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 **ip sla 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.

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

ip sla logging traps

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 **ip sla logging traps** command in global configuration mode. To disable IP SLAs system logging SNMP traps, use the **no** form of this command.

ip sla logging traps

no ip sla 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
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor logging traps** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr logging traps** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor logging traps** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor logging traps** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

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 **ip sla 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:

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

Related Commands

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

ip sla low-memory

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

ip sla low-memory *bytes*

no ip sla low-memory

Syntax Description

bytes	Specifies amount of memory, in bytes, that must be available to configure IP SLA. The range is from 0 to the maximum amount of free memory bytes available.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor low-memory** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr low-memory** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor low-memory** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor low-memory** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

The **ip sla low-memory** command allows you to specify the amount of memory that the IP SLAs can use. If the amount of available free memory falls below the value specified in the **ip sla low-memory** command, then the IP SLAs will not allow new operations to be configured. 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 **ip sla 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** user EXEC or privileged 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:

```
ip sla low-memory 2097152
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
show memory	Displays statistics about memory, including memory-free pool statistics.

ip sla monitor

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor** command is replaced by the **ip sla** command. See the **ip sla** command for more information.

To begin configuring a Cisco IOS IP Service Level Agreements (SLAs) operation and enter IP SLA monitor configuration mode, use the **ip sla monitor** 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.

ip sla monitor *operation-number*

no ip sla monitor *operation-number*

Syntax Description

operation-number	Operation number used for the identification of the IP SLAs operation you want to configure.

Defaults

No IP SLAs operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla** command.
12.2(33)SXI	This command was replaced by the **ip sla** command.

Usage Guidelines

The **ip sla monitor** command is used to begin configuration for an IP SLAs operation. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, the router will enter IP SLA monitor configuration mode.

IP SLAs allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

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

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

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 ip sla monitor** command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show ip sla monitor configuration** command in user EXEC or privileged EXEC mode.

Examples

In the following example, operation 99 is configured as a UDP jitter operation and scheduled to start running in 5 hours:

```
ip sla monitor 99
 type jitter dest-ipaddr 172.29.139.134 dest-port 5000 num-packets 20
!
ip sla monitor schedule 99 life 300 start-time after 00:05:00
```

Note If operation 99 already exists and has not been scheduled, the command line interface will enter IP SLA monitor configuration mode for operation 99. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
ip sla monitor group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
ip sla monitor reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
ip sla monitor 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.
ip sla monitor schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show ip sla monitor statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla monitor statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

ip sla monitor group schedule

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor group schedule** command is replaced by the **ip sla group schedule** command. See the **ip sla group schedule** command for more information.

To perform group scheduling for Cisco IOS IP Service Level Agreements (SLAs) operations, use the **ip sla monitor 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.

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

no ip sla monitor group schedule

Syntax Description

group-operation-number	Group configuration or group schedule number of the IP SLAs operation to be scheduled. The range is from 0 to 65535.
operation-id-numbers	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: • 2, 3, 4, 9, 20 • 10-20, 30-35, 60-70 • 2, 3, 4, 90-100, 105-115 The *operation-id-numbers* argument can include a maximum of 125 characters.
schedule-period *seconds*	Specifies the time (in seconds) for which the IP SLAs operation group is scheduled. The range is from 1 to 604800.
ageout *seconds*	(Optional) Specifies the number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 (never ages out).
frequency *seconds*	(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.

frequency range *random-frequency-range*	(Optional) Enables the random scheduler option. The random scheduler option is disabled by default. The uniformly distributed random frequencies at which the group of operations will restart is chosen within the specified frequency range (in seconds). Separate the lower and upper frequency values with a hyphen (for example, 80-100).
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Specifies the number of seconds the operation actively collects information. The default is 3600 (one hour).
start-time	(Optional) Specifies the 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**.
hh:*mm*[:*ss*]	(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 *month* and *day*.
month	(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. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) 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.
pending	(Optional) Indicates that no information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after *hh*:*mm*:*ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* 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(14)T	This command was introduced.
12.4(2)T	The **range** keyword and *random-frequency-range* argument were introduced.
12.4(4)T	This command was replaced by the **ip sla group schedule** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr group schedule** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.2(33)SB	This command was replaced by the **ip sla group schedule** command.
12.2(33)SXI	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 any significant CPU impact.

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:

ip sla monitor group schedule 2 1-780 schedule-period 60 start-time 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.

On a Cisco 2600 router, the maximum recommended value of operations per second is 6 or 7 (approximately 350 to 400 operations per minute). Exceeding this value of 6 or 7 operations per second could cause major performance (CPU) impact. Note that the maximum recommended value of operations per second varies from platform to platform.

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:

ip sla monitor 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.

IP SLAs Random Scheduler

The IP SLAs random scheduler option provides the capability to schedule multiple IP SLAs operations to begin at random intervals over a specified duration of time. The random scheduler option is disabled by default. To enable the random scheduler option, you must configure the **frequency range** *random-frequency-range* keywords and argument. The group of operations restarts at uniformly distributed random frequencies within the specified frequency range. The following guidelines apply for setting the frequency range:

- The starting value of the frequency range should be greater than the timeout values of all the operations in the group operation.
- The starting value of the frequency range should be greater than the schedule period (amount of time for which the group operation is scheduled). This guideline ensures that the same operation does not get scheduled more than once within the schedule period.

The following guidelines apply if the random scheduler option is enabled:

- The individual operations in a group operation will be uniformly distributed to begin at random intervals over the schedule period.
- The group of operations restarts at uniformly distributed random frequencies within the specified frequency range.
- The minimum time interval between the start of each operation in a group operation is 100 milliseconds (0.1 seconds). If the random scheduler option is disabled, the minimum time interval is 1 second.
- Only one operation can be scheduled to begin at any given time. If the random scheduler option is disabled, multiple operations can begin at the same time.
- The first operation will always begin at 0 milliseconds of the schedule period.
- The order in which each operation in a group operation begins is random.

Examples

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 as a group (identified as group 1). In this example, the operations are scheduled to begin at equal intervals over a schedule period of 20 seconds. The first operation (or set of operations) is scheduled to start immediately. Since the frequency is not specified, it is set to the value of the schedule period (20 seconds) by default.

```
ip sla monitor group schedule 1 3, 4, 6-10 schedule-period 20 start-time now
```

The following example shows how to schedule IP SLAs operations 1 to 3 as a group (identified as group 2). In this example, the operations are scheduled to begin at random intervals over a schedule period of 50 seconds. The first operation is scheduled to start immediately. The random scheduler option is enabled and the frequency at which the group of operations will restart will be chosen randomly within the range of 80-100 seconds.

```
ip sla monitor group schedule 2 1-3 schedule-period 50 frequency range 80-100 start-time
now
```

Related Commands

Command	Description
ip sla monitor schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla monitor configuration	Displays the configuration details of the IP SLAs operation.
show ip sla monitor group schedule	Displays the group scheduling details of the IP SLAs operations.

ip sla monitor key-chain

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor key-chain** command is replaced by the **ip sla key-chain** command. See the **ip sla key-chain** command for more information.

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

ip sla monitor key-chain *name*

no ip sla monitor key-chain

Syntax Description

name	Name of MD5 key chain.

Defaults

Control message authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla key-chain** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr key-chain** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla key-chain** command.
12.2(33)SXI	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 **ip sla monitor 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.

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

ip sla monitor logging traps

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor logging traps** command is replaced by the **ip sla logging traps** command. See the **ip sla logging traps** command 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 **ip sla monitor logging traps** command in global configuration mode. To disable IP SLAs system logging SNMP traps, use the **no** form of this command.

ip sla monitor logging traps

no ip sla monitor 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(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla logging traps** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr logging traps** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla logging traps** command.
12.2(33)SXI	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 **ip sla monitor 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:

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

Related Commands

Command	Description
ip sla monitor reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.
snmp-server enable traps rtr	Enables the sending of IP SLAs SNMP trap notifications.

ip sla monitor low-memory

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor low-memory** command is replaced by the **ip sla low-memory** command. See the **ip sla low-memory** command for more information.

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

ip sla monitor low-memory *bytes*

no ip sla monitor low-memory

Syntax Description

bytes	Specifies amount of memory, in bytes, that must be available to configure IP SLA. The range is from 0 to the maximum amount of free memory bytes available.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla low-memory** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr low-memory** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla low-memory** command.
12.2(33)SXI	This command was replaced by the **ip sla low-memory** command.

Usage Guidelines

The **ip sla monitor low-memory** command allows you to specify the amount of memory that the IP SLAs can use. If the amount of available free memory falls below the value specified in the **ip sla monitor low-memory** command, then the IP SLAs will not allow new operations to be configured. 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 **ip sla monitor 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** user EXEC or privileged 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:

```
ip sla monitor low-memory 2097152
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
show memory	Displays statistics about memory, including memory-free pool statistics.

ip sla monitor reaction-configuration

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor reaction-configuration** command is replaced by the **ip sla reaction-configuration** command. See the **ip sla reaction-configuration** command for more information.

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **ip sla monitor 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.

ip sla monitor reaction-configuration *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]

no ip sla monitor reaction-configuration *operation-number*

Syntax Description

operation-number	Number of the IP SLAs operation for which reactions are to be configured.
react *monitored-element*	Specifies the element to be monitored for threshold violations. **Note** The elements available for monitoring will vary depending on the type of IP SLAs operation you are configuring. Keyword options for the monitored-element argument are as follows: • **connectionLoss**—Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. • **icpif**—Specifies that a reaction should occur if the one-way Calculated Planning Impairment Factor (ICPIF) value violates the upper threshold or lower threshold. • **jitterAvg**—Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg**—Specifies that a reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg**—Specifies that a reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold.

react *monitored-element* (continued)	• **maxOfNegativeDS**—Specifies that a reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD**—Specifies that a reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated. • **maxOfPositiveDS**—Specifies that a reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD**—Specifies that a reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated. • **mos**—Specifies that a reaction should occur if the one-way mean opinion score (MOS) value violates the upper threshold or lower threshold. • **packetLateArrival**—Specifies that a reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLossDS**—Specifies that a reaction should occur if the one-way destination-to-source packet loss value violates the upper threshold or lower threshold. • **packetLossSD**—Specifies that a reaction should occur if the one-way source-to-destination packet loss value violates the upper threshold or lower threshold. • **packetMIA**—Specifies that a reaction should occur if the one-way number of missing packets violates the upper threshold or lower threshold. • **packetOutOfSequence**—Specifies that a reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt**—Specifies that a reaction should occur if the round-trip time violates the upper threshold or lower threshold. • **timeout**—Specifies that a reaction should occur if there is a one-way timeout for the monitored operation. • **verifyError**—Specifies that a reaction should occur if there is a one-way error verification violation.

action-type *option*	(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 *option* argument can be one of the following keywords: • **none**—No action is taken. This option is the default value. • **trapAndTrigger**—Trigger an Simple Network Management Protocol (SNMP) trap and start another IP SLAs operation when the violation conditions are met, as defined in the **trapOnly** and **triggerOnly** options. • **trapOnly**—Send an SNMP logging trap when the specified violation type occurs for the monitored element. • **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 **ip sla monitor 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.
threshold-type average [*number-of-measurements*]	(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the **action-type** keyword. 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. The default number of 5 averaged measurements can be changed using the *number-of-measurements* argument. The valid range is from 1 to 16. This syntax is not available if the **connectionLoss**, **timeout**, or **verifyError** keyword is specified as the monitored element, because upper and lower thresholds do not apply to these options.
threshold-type consecutive [*occurrences*]	(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 *occurrences* argument. The valid range is from 1 to 16. The *occurrences* value will appear in the output of the **show ip sla monitor reaction-configuration** command as the "Threshold Count" value.
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 is the default threshold type.

threshold-type xofy [*x-value y-value*]	(Optional) When a threshold violations for the monitored element is met *x* number of times within the last *y* number of measurements ("x of y"), perform the action defined by the **action-type** keyword. The default is 5 for both the x and y values (**xofy 5 5**). The valid range for each value is from 1 to 16. The *x-value* will appear in the output of the **show ip sla monitor reaction-configuration** command as the "Threshold Count" value, and the *y-value* will appear as the "Threshold Count2" value.
[**threshold-value** *upper-threshold lower-threshold*]	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See Table 10 in the "Usage Guidelines" section for a list of the default values. **Note** For MOS threshold values (**react mos**), the number is expressed in three 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).

Defaults

IP SLAs proactive threshold monitoring is disabled.

Note See Table 11 in the "Usage Guidelines" section for a list of the default upper and lower thresholds for specific monitored elements.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	The following keywords for the *monitored-element* argument were added: • **icpif** • **maxOfNegativeDS** • **maxOfPositiveDS** • **maxOfNegativeSD** • **maxOfPositiveSD** • **packetLateArrival** • **packetMIA** • **packetOutOfSequence**
12.4(4)T	This command was replaced by the **ip sla reaction-configuration** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr reaction-configuration** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla reaction-configuration** command.
12.2(33)SXI	This command was replaced by the **ip sla reaction-configuration** command.

Usage Guidelines

You can configure the **ip sla monitor 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 ip sla monitor reaction-configuration** command will disable all proactive threshold monitoring configuration for the specified IP SLAs operation.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **ip sla monitor logging traps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-server enable traps rtr** command to enable the sending of IP SLAs SNMP trap notifications.

To display the current threshold monitoring configuration settings for an IP SLAs operation, use the **show ip sla monitor configuration** command.

Table 11 lists the default upper and lower thresholds for specific monitored elements.

Table 11 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms
jitterSDAvg	100 ms	100 ms
maxOfNegativeDS	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
mos	500 (score)	100 (score)
packetLateArrival	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rtt	5000 ms	3000 ms

Examples

In the following example, IP SLAs operation 10 (a UDP 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):

```
ip sla monitor reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla monitor logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
ip sla monitor 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** global configuration command.
show ip sla monitor reaction-configuration	Displays the configured proactive threshold monitoring settings for all IP SLAs operations or a specified operation.
show ip sla monitor reaction-trigger	Displays the configured state of triggered IP SLAs operations.
snmp-server enable traps rtr	Enables the sending of IP SLAs SNMP trap notifications.

ip sla monitor reaction-trigger

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor reaction-trigger** command is replaced by the **ip sla reaction-trigger** command. See the **ip sla reaction-trigger** command for more information.

To define a second Cisco IOS IP Service Level Agreements (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, use the **ip sla monitor reaction-trigger** command in global configuration mode. To remove the trigger combination, use the **no** form of this command.

ip sla monitor reaction-trigger *operation-number target-operation*

no ip sla monitor reaction-trigger *operation*

Syntax Description

operation-number	Number of the operation for which a trigger action type is defined (using the **ip sla monitor reaction-configuration** global configuration command).
target-operation	Number of the operation that will be triggered into an active state.

Defaults

No trigger combination is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla reaction-trigger** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr reaction-trigger** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla reaction-trigger** command.
12.2(33)SXI	This command was replaced by the **ip sla reaction-trigger** command.

Usage Guidelines

Triggers are usually used for diagnostics purposes and are not intended for use during normal operation conditions.

Examples

In the following example, a trigger action type is defined for IP SLAs operation 2. When operation 2 experiences certain user-specified threshold violation events while it is actively collecting statistical information, the operation state of IP SLAs operation 1 will be triggered to change from pending to active.

```
ip sla monitor reaction-trigger 2 1
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla monitor reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLA.
ip sla monitor schedule	Configures the time parameters for an IP SLAs operation.

ip sla monitor reset

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor reset** command is replaced by the **ip sla reset** command. See the **ip sla reset** command for more information.

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

ip sla monitor reset

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla reset** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr reset** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla reset** command.
12.2(33)SXI	This command was replaced by the **ip sla reset** command.

Usage Guidelines

The **ip sla monitor 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 the startup configuration in NVRAM. You must retype the configuration or load a previously saved configuration file.

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

Note Use the **ip sla monitor reset** command only in extreme situations such as the incorrect configuration of a number of operations.

Examples

The following example shows how to reset the Cisco IOS IP SLAs engine, clearing all stored IP SLAs information and configuration:

```
ip sla monitor reset
```

Related Commands

Command	Description
ip sla monitor restart	Restarts a stopped IP SLAs operation.

ip sla monitor responder

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor responder** command is replaced by the **ip sla responder** command. See the **ip sla responder** command for more information.

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for general IP SLAs operations, use the **ip sla monitor responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

ip sla monitor responder

no ip sla monitor responder

Syntax Description

This command has no arguments or keywords.

Defaults

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla responder** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr responder** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla responder** command.
12.2(33)SXI	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 and receiving of IP SLAs control packets. Enabling the IP SLAs Responder allows the generation of packet loss statistics on the device sending IP SLAs operations.

Prior to sending an operation packet to the IP SLAs Responder, the IP SLAs operation sends a control message to the IP SLAs Responder to enable the destination port.

Examples

The following example shows how to enable the IP SLAs Responder:

```
ip sla monitor responder
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla monitor responder type tcpConnect ipaddress	Enables the IP SLAs Responder for TCP Connect operations.
ip sla monitor responder type udpEcho ipaddress	Enables the IP SLAs Responder for UDP echo and jitter operations.

ip sla monitor responder type tcpConnect ipaddress

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor responder type tcpConnect ipaddress** command is replaced by the **ip sla responder tcp-connect ipaddress** command. See the **ip sla responder tcp-connect ipaddress** command for more information.

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

ip sla monitor responder type tcpConnect ipaddress *ip-address* **port** *port-number*

no ip sla monitor responder type tcpConnect ipaddress *ip-address* **port** *port-number*

Syntax Description

ip-address	Destination IP address.
port *port-number*	Specifies the destination port number.

Defaults

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla responder tcp-connect ipaddress** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr responder type tcpConnect** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla responder tcp-connect ipaddress** command.
12.2(33)SXI	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 connection operation packets.

Examples

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

```
ip sla monitor responder type tcpConnect ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla monitor responder	Enables the IP SLAs Responder for nonspecific IP SLAs operations.

ip sla monitor responder type udpEcho ipaddress

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor responder type udpEcho ipaddress** command is replaced by the **ip sla responder udp-echo ipaddress** command. See the **ip sla responder udp-echo ipaddress** command for more information.

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for User Datagram Protocol (UDP) echo or jitter operations, use the **ip sla monitor responder type udpEcho ipaddress** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

ip sla monitor responder type udpEcho ipaddress *ip-address* **port** *port-number*

no ip sla monitor responder type udpEcho ipaddress *ip-address* **port** *port-number*

Syntax Description

ip-address	Destination IP address.
port *port-number*	Specifies the destination port number.

Defaults

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla responder udp-echo ipaddress** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr responder type udpEcho** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla responder udp-echo ipaddress** command.
12.2(33)SXI	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 UDP echo and jitter (UDP+) operations with control disabled.

Examples

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

```
ip sla monitor responder type udpEcho ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla monitor responder	Enables the IP SLAs Responder for nonspecific IP SLAs operations.

ip sla monitor restart

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor restart** command is replaced by the **ip sla restart** command. See the **ip sla restart** command for more information.

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

ip sla monitor restart *operation-number*

Syntax Description

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

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla restart** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr restart** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla restart** command.
12.2(33)SXI	This command was replaced by the **ip sla restart** command.

Usage Guidelines

To restart an operation, the operation should be in an active state.

IP SLAs allows a maximum of 2000 operations.

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

Examples

The following example shows how to restart operation 12:

```
ip sla monitor restart 12
```

Related Commands

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

ip sla monitor schedule

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **ip sla monitor schedule** command is replaced by the **ip sla schedule** command. See the **ip sla schedule** command for more information.

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

ip sla monitor schedule *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no ip sla monitor schedule *operation-number*

Syntax Description

operation-number	Number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts.
hh:*mm*[:*ss*]	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 *month* and *day*.
month	(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. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) 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.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after *hh*:*mm*:*ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
ageout *seconds*	(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
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **ip sla schedule** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtr schedule** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **ip sla schedule** command.
12.2(33)SXI	This command was replaced by the **ip sla schedule** command.

Usage Guidelines After you schedule the operation with the **ip sla monitor schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the **ip sla monitor** 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 **ip sla monitor reaction-trigger** and **ip sla monitor 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 **ip sla monitor** 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 **ip sla monitor 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.

The operation to can age out before it executes (that is, Z can occur before X). To ensure that this does not happen, configure the difference between the operation’s configuration time and start time (X and W) to 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 supported only for scheduling single IP SLAs operations. You cannot schedule multiple IP SLAs operations using the **ip sla monitor 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 configuration in RAM).

```
ip sla monitor 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:

```
ip sla monitor schedule 1 start-time after 00:05:00
```

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

```
ip sla monitor schedule 3 start-time now life forever
```

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

```
ip sla monitor schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla monitor group schedule	Performs group scheduling for IP SLAs operations.
ip sla monitor reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLA.
ip sla monitor 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 **ip sla monitor reaction-configuration** global configuration command.
show ip sla monitor configuration	Displays the configuration details of the IP SLAs operation.

ip sla reaction-configuration

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

ip sla reaction-configuration *operation-number* [**react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]

no ip sla reaction-configuration *operation-number* [**react** *monitored-element*]

Syntax Description

operation-number	Number of the IP SLAs operation for which reactions are to be configured.
react *monitored-element*	(Optional) Specifies the element to be monitored for threshold violations. **Note** The elements supported for monitoring will vary depending on the type of IP SLAs operation you are running. See the Usage Guidelines for information. Keyword options for the *monitored-element* argument are as follows: • **connectionLoss**—Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **frameLossDS**—Specifies that a reaction should occur if the one-way destination-to-source digital signal processor (DSP) frame loss value violates the upper threshold or lower threshold. • **iaJitterDS**—Specifies that a reaction should occur if the one-way destination-to-source interarrival jitter value violates the upper threshold or lower threshold. • **iaJitterSD**—Specifies that a reaction should occur if the one-way source-to-destination interarrival jitter value violates the upper threshold or lower threshold. • **icpif**—Specifies that a reaction should occur if the one-way Calculated Planning Impairment Factor (ICPIF) value violates the upper threshold or lower threshold. • **jitterAvg**—Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg**—Specifies that a reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg**—Specifies that a reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold.

react *monitored-element* (continued)	• **latencyDSAvg**—Specifies that a reaction should occur if the average one-way destination-to-source latency value violates the upper threshold or lower threshold. • **latencySDAvg**—Specifies that a reaction should occur if the average one-way source-to-destination latency value violates the upper threshold or lower threshold. • **maxOflatencyDS**—Specifies that a reaction should occur if the one-way maximum latency destination-to-source threshold is violated. • **maxOflatencySD**—Specifies that a reaction should occur if the one-way maximum latency source-to-destination threshold is violated. • **maxOfNegativeDS**—Specifies that a reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD**—Specifies that a reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated. • **maxOfPositiveDS**—Specifies that a reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD**—Specifies that a reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated. • **mos**—Specifies that a reaction should occur if the one-way Mean Opinion Score (MOS) value violates the upper threshold or lower threshold. • **moscqds**—Specifies that a reaction should occur if the one-way destination-to-source Mean Opinion Score for Conversational Quality (MOS-CQ) value violates the upper threshold or lower threshold. • **moscqsd**—Specifies that a reaction should occur if the one-way source-to-destination Mean Opinion Score for Conversational Quality (MOS-CQ) value violates the upper threshold or lower threshold. • **moslqds**—Specifies that a reaction should occur if the one-way destination-to-source Mean Opinion Score for Listening Quality (MOS-LQ) value violates the upper threshold or lower threshold. • **packetLateArrival**—Specifies that a reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold.

react *monitored-element* (continued)	• **packetLoss**—Specifies that a reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetLossDS**—Specifies that a reaction should occur if the one-way destination-to-source packet loss value violates the upper threshold or lower threshold. • **packetLossSD**—Specifies that a reaction should occur if the one-way source-to-destination packet loss value violates the upper threshold or lower threshold. • **packetMIA**—Specifies that a reaction should occur if the one-way number of missing packets violates the upper threshold or lower threshold. • **packetOutOfSequence**—Specifies that a reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rFactorDS**—Specifies that a reaction should occur if the one-way destination-to-source estimated transmission rating factor R violates the upper threshold or lower threshold. • **rFactorSD**—Specifies that a reaction should occur if the one-way source-to-destination estimated transmission rating factor R violates the upper threshold or lower threshold. • **rtt**—Specifies that a reaction should occur if the round-trip time violates the upper threshold or lower threshold. • **successivePacketLoss**—Specifies that a reaction should occur if the one-way number of successively dropped packets violates the upper threshold or lower threshold. • **timeout**—Specifies that a reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError**—Specifies that a reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.

action-type *option*	(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 *option* argument can be one of the following keywords: • **none**—No action is taken. This option is the default value. • **trapAndTrigger**—Trigger a Simple Network Management Protocol (SNMP) trap and start another IP SLAs operation when the violation conditions are met, as defined in the **trapOnly** and **triggerOnly** options. • **trapOnly**—Send an SNMP logging trap when the specified violation type occurs for the monitored element. • **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 **ip sla 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.
threshold-type average [*number-of-measurements*]	(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the **action-type** keyword. 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. The default number of 5 averaged measurements can be changed using the *number-of-measurements* argument. The valid range is from 1 to 16. This syntax is not available if the **connectionLoss**, **timeout**, or **verifyError** keyword is specified as the monitored element, because upper and lower thresholds do not apply to these options.
threshold-type consecutive [*occurrences*]	(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 *occurrences* argument. The valid range is from 1 to 16. The *occurrences* value will appear in the output of the **show ip sla reaction-configuration** command as the "Threshold Count" value.
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 is the default threshold type.

threshold-type xofy [*x-value y-value*]	(Optional) When a threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements (“x of y”), perform the action defined by the **action-type** keyword. The default is 5 for both the x and y values (**xofy 5 5**). The valid range for each value is from 1 to 16. The *x-value* will appear in the output of the **show ip sla reaction-configuration** command as the “Threshold Count” value, and the *y-value* will appear as the “Threshold Count2” value.
threshold-value *upper-threshold lower-threshold*	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See Table 15 in the “Usage Guidelines” section for a list of the default values. **Note** For MOS threshold values (**react mos**), the number is expressed in three 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).

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor reaction-configuration** command. The following keywords for the *monitored-element* argument were added to support the IP SLAs RTP-based VoIP operation: • **frameLossDS** • **iaJitterDS** • **moscqds** • **moslqds** • **rFactorDS**

Release	Modification
12.4(6)T	This command was modified. The following keywords for the *monitored-element* argument were added to support the IP SLAs ICMP jitter and IP SLAs RTP-based VoIP operations: • **iaJitterSD** • **latencyDSAvg** • **latencySDAvg** • **maxOflatencyDS** • **maxOflatencySD** • **moscqsd** • **packetLoss** • **rFactorSD** • **successivePacketLoss**
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr reaction-configuration** command. The following keywords for the *monitored-element* argument were added: • **icpif** • **maxOfNegativeDS** • **maxOfPositiveDS** • **maxOfNegativeSD** • **maxOfPositiveSD** • **packetLateArrival** • **packetMIA** • **packetOutOfSequence**
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor reaction-configuration** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor reaction-configuration** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

You can configure the **ip sla reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements, such as configuring thresholds for both destination-to-source packet loss and MOS for the same operation. However, disabling individual monitored elements is not supported. The **no ip sla reaction-configuration** command disables all proactive threshold monitoring configuration for the specified IP SLAs operation.

The keyword options for this command are not case sensitive. The keywords in online help for the **action-type** *option* and **react** *monitored-element* keyword and argument combinations contain uppercase letters to enhance readability only.

Not all elements can be monitored by all IP SLAs operations. If you attempt to configure an unsupported *monitored-element*, such as MOS for a UDP echo operation, the following message displays:

```
Invalid react option for the Probe type configured
```

Before Cisco IOS Release 15.1(1)T, valid online help was not available for this command. See Table 12 and Table 13 for a list of elements that are supported for each IP SLA operation.

In Cisco IOS Release 15.1(1)T and later releases, type **shift + ?** to display a list of supported elements for the IP SLAs operation being configured.

Table 12 Supported Elements, by IP SLA Operation

monitored-element	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
failure	Y	—	Y	Y	Y	Y	—	Y	Y	—
rtt	Y	Y	—	Y	Y	Y	Y	—	Y	Y
RTTAvg	—	—	Y	—	—	—	—	Y	—	—
timeout	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
connectionLoss	—	—	Y	Y	Y	—	—	—	—	
verifyError	—	—	Y	Y	—	—	—	Y	—	Y
jitterSDAvg	—	—	Y	—	—	—		Y	—	—
jitterAvg	—	—	Y	—	—	—	—	Y	—	—
packetLateArrival	—	—	Y	—	—	—	—	Y	—	—
packetOutOfSequence	—	—	Y	—	—	—	—	Y	—	—
maxOfPostiveSD	—	—	Y	—	—	—		Y	—	—
maxOfNegativeSD	—	—	Y	—	—	—	—	Y	—	—
maxOfPostiveDS	—	—	Y	—	—	—	—	Y	—	—
maxOfNegativeDS	—	—	Y	—	—	—	—	Y	—	—
mos	—	—	Y	—	—	—		—	—	—
icpif	—	—	Y	—	—	—	—	—	—	—
packetLossDS	—	—	Y	—	—	—	—	—	—	—
packetLossSD	—	—	Y	—	—	—	—	—	—	—
packetMIA	—	—	Y	—	—	—		—	—	—
iaJitterDS	—	—	—	—	—	—	—	—	—	—
frameLossDS	—	—	—	—	—	—	—	—	—	—
mosLQDS	—	—	—	—	—	—	—	—	—	—
mosCQDS	—	—	—	—	—	—	—	—	—	—
rfactorDS	—	—	—	—	—	—	—	—	—	—
iaJitterSD	—	—	—	—	—	—	—	—	—	—
successivePacketLoss	—	—	—	—	—	—	—	Y	—	—
maxOfLatencyDS	—	—	—	—	—	—	—	Y	—	—
maxOfLatencySD	—	—	—	—	—	—	—	Y	—	—
latencyDS	—	—	—	—	—	—	—	Y	—	—

Table 12 Supported Elements, by IP SLA Operation (continued)

monitored-element	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
latencySD	—	—	—	—	—	—	—	Y	—	—
packetLoss	—	—	—	—	—	—	—	Y	—	—

Table 13 Supported Elements, by IP SLA Operation

Monitored Element	HTTP	SLM	RTP	FTP	LSP Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
failure	—	—	—	—	—	—	—	—	—
rtt	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTTAvg	—	—	—	—	—	—	—	—	—
timeout	Y	Y	Y	Y	—	Y	Y	Y	Y
connectionLoss	Y		Y	Y	Y	—	—	Y	—
verifyError	—	—	—	—	—	—	—	—	—
jitterSDAvg	—	—	—	—	—	—	Y	—	—
jitterAvg	—	—	—	—	—	—	Y	—	—
packetLateArrival	—	—	—	—	—	—	Y	—	—
packetOutOfSequence	—	—	—	—	—	—	Y	—	—
maxOfPostiveSD	—	—	—	—	—	—	Y	—	—
maxOfNegativeSD	—	—	—	—	—	—	Y	—	—
maxOfPostiveDS	—	—	—	—	—	—	Y	—	—
maxOfNegativeDS	—	—	—	—	—	—	Y	—	—
mos	—	—	—	—	—	—	—	—	—
icpif	—	—	—	—	—	—	—	—	—
packetLossDS	—	—	Y	—	—	—	—	—	—
packetLossSD	—	—	Y	—	—	—	—	—	—
packetMIA	—	—	Y	—	—	—	—	—	—
iaJitterDS	—	—	Y	—	—	—	—	—	—
frameLossDS	—	—	Y	—	—	—	—	—	—
mosLQDSS	—	—	Y	—	—	—	—	—	—
mosCQDS	—	—	Y	—	—	—	—	—	—
rfactorDS	—	—	Y						
iaJitterSD	—	—	Y	—	—	—	—	—	—
successivePacketLoss	—	—	—	—	—	—	—	—	—
maxOfLatencyDS	—	—	—	—	—	—	—	—	—
maxOfLatencySD	—	—	—	—	—	—	—	—	—
latencyDS	—	—	—	—	—	—	—	—	—

Table 13 Supported Elements, by IP SLA Operation (continued)

Monitored Element	HTTP	SLM	RTP	FTP	LSP Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
latencySD	—	—	—	—	—	—	—	—	—
packetLoss	—	—	—	—	—	—	—	—	—

Return-trip time (RTT) reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT). SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation.

The connectionLoss trap is sent if the control connection is established and the operation is running, then the IP SLAs responder process stops, for example, if the **no ip sla responder** command is issued. This trap is supported only by operations that use the IPSLA control protocol to establish a control connection, such as udp-jitter and udp-echo. ICMP operations do not support connectionLoss traps.

lists the action or combination of actions that are supported when a threshold event for a monitored element occurs.

Table 14 Supported Action Type for Threshold Events

Threshold Event	Generate Syslog Messages	Trigger SNMP Trap
RTT violations during jitter operations	Y	Unsupported
RTT violations during non-jitter operations	Unsupported	Y
Non-RTT violations other than timeout, connectLoss, or verifyError	Y	Unsupported
timeout violations	Y	Y
connectionLoss violations	Y	Y
verifyError violations	Y	Y

Use the **snmp-server enable traps rtr** or **snmp-server enable traps syslog** command to enable the sending of IP SLAs SNMP trap notifications.

Use the **ip sla logging traps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications.

Table 15 lists the default upper and lower thresholds for specific monitored elements.

Table 15 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
frameLossDS	1000 frames	1000 frames
iaJitterDS	20 ms	20 ms
iaJitterSD	20 ms	20 ms
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms

Table 15 Default Threshold Values for Monitored Elements (continued)

Monitored Element Keyword	Upper Threshold	Lower Threshold
jitterSDAvg	100 ms	100 ms
latencyDSAvg	5000 ms	3000 ms
latencySDAvg	5000 ms	3000 ms
maxOflatencyDS	5000 ms	3000 ms
maxOflatencySD	5000 ms	3000 ms
maxOfNegativeDS	10000 ms	10000 ms
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
mos	500 (score)	100 (score)
moscqds	410 (score)	310 (score)
moscqsd	410 (score)	310 (score)
moslqds	410 (score)	310 (score)
packetLateArrival	10000 packets	10000 packets
packetLoss	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rFactorDS	80	60
rFactorSD	80	60
rtt	5000 ms	3000 ms
successivePacketLoss	10000 packets	10000 packets

To display the current threshold monitoring configuration settings for an IP SLAs operation, use the **show ip sla configuration** command.

Examples

The following example shows how to configure IP SLAs operation 10 (a UDP jitter operation) to send an SNMP logging trap when the MOS value exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
Router(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
ip sla 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 reaction-configuration** global configuration command.
no ip sla responder	Disables the IP SLAs responder on the destination device.
show ip sla reaction-configuration	Displays the configured proactive threshold monitoring settings for all IP SLAs operations or a specified operation.
show ip sla reaction-trigger	Displays the configured state of triggered IP SLAs operations.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

ip sla reaction-trigger

To define a second Cisco IOS IP Service Level Agreements (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 reaction-configuration** command, use the **ip sla reaction-trigger** command in global configuration mode. To remove the trigger combination, use the **no** form of this command.

ip sla reaction-trigger *operation-number target-operation*

no ip sla reaction-trigger *operation*

Syntax Description

operation-number	Number of the operation for which a trigger action type is defined (using the **ip sla reaction-configuration** global configuration command).
target-operation	Number of the operation that will be triggered into an active state.

Defaults

No trigger combination is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor reaction-trigger** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr reaction-trigger** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor reaction-trigger** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor reaction-trigger** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

Triggers are usually used for diagnostics purposes and are not intended for use during normal operation conditions.

Examples

In the following example, a trigger action type is defined for IP SLAs operation 2. When operation 2 experiences certain user-specified threshold violation events while it is actively collecting statistical information, the operation state of IP SLAs operation 1 will be triggered to change from pending to active.

```
ip sla reaction-trigger 2 1
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLA.
ip sla schedule	Configures the time parameters for an IP SLAs operation.

ip sla reset

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

ip sla reset

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor reset** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr reset** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor reset** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor reset** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

The **ip sla reset** command stops all IP SLAs 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 the startup configuration in NVRAM. You must retype the configuration or load a previously saved configuration file.

Note The **ip sla reset** command does not remove IP SLAs label switched path (LSP) Health Monitor configurations from the running configuration. Use the **auto ip sla mpls-lsp-monitor reset** command to remove LSP Health Monitor configurations from the running configuration.

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

Examples

The following example shows how to reset the Cisco IOS IP SLAs engine, clearing all stored IP SLAs information and configuration:

```
ip sla reset
```

Related Commands

Command	Description
ip sla restart	Restarts a stopped IP SLAs operation.

ip sla responder

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for general IP SLAs operations, use the **ip sla responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

ip sla responder

no ip sla responder

Syntax Description

This command has no arguments or keywords.

Defaults

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor responder** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr responder** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor responder** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor responder** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

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

Prior to sending an operation packet to the IP SLAs Responder, the IP SLAs operation sends a control message to the IP SLAs Responder to enable the destination port.

The **ip sla responder** command is supported in IPv4 networks. This command can also be used when configuring an IP SLAs operation that supports IPv6 addresses.

Examples

The following example shows how to enable the IP SLAs Responder:

```
ip sla responder
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla responder type tcpConnect ipaddress	Enables the IP SLAs Responder for TCP Connect operations.
ip sla responder type udpEcho ipaddress	Enables the IP SLAs Responder for UDP echo and jitter operations.

ip sla responder auto-register

To configure a destination Cisco routing device or Cisco IP Service Level Agreements (SLAs) Responder to automatically register with the source upon configuration, use the **ip sla responder auto-register** command in global configuration mode. To disable automatic registration, use the **no** form of this command.

ip sla responder auto-register {*source-ipaddress* | *source-hostname*} [**client-id** *client-id*] [**endpoint-list** *template-name*] [**retry-timer** *minutes*]

no ip sla responder auto-register {*source-ipaddress* | *source-hostname*} [**client-id** *client-id*] [**endpoint-list** *template-name*] [**retry-timer** *minutes*]

Syntax Description

source-ipaddress	Specifies IP address of source for IP SLAs operation.
source-hostname	Specifies hostname of source for IP SLAs operation.
client-id	(Optional) Specifies unique identifier for this responder.
client-id	String of 1 to 64 alphanumeric characters.
endpoint-list	(Optional) Specifies unique identifier of auto IP SLAs endpoint list to which this responder will be added during auto discovery.
template-name	String of 1 to 64 ASCII characters.
retry-timer	(Optional) Specifies the length of time before responder attempts to register again, in minutes.
minutes	Range is from 1 to 1440. Default is 3 minutes.

Command Default

The Cisco IP SLAs Responder does not automatically register with source.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command is required to allow the Cisco destination routing device or Cisco IP SLAs Responder to automatically register with the source and enable the source to automatically discover the endpoint.

Examples

The following example shows how to configure this command to enable auto discovery for configuring an auto IP SLAs endpoint list:

Destination

```
Router(config)# ip sla responder auto-register 10.1.1.23 endpoint-list autolist
Router(config)# exit
Router#
```

Source

```
Router(config)#ip sla auto discover
Router(config)#ip sla auto endpoint-list type ip autolist
Router(config-epl)#discover port 5000
Router(config-epl)#access-list 3
Router(config-term)#exit
Router# show ip sla auto endpoint-list
Endpoint-list Name: autolist
    Description:
    Auto Discover Parameters
        Destination Port: 5000
        Access-list: 3
        Ageout: 3600    Measurement-retry: 3

    1 endpoints are discovered for autolist
```

Related Commands

Command	Description
destination (am-group)	Specifies an endpoint list for an IP SLAs auto-measure group.
discover (epl)	Enters IP SLA endpoint-list auto-discovery configuration mode for building an auto IP SLAs endpoint list using auto discovery.
ip sla auto endpoint-list	Begins configuration for an auto IP SLAs endpoint list and enters IP SLA endpoint-list configuration mode.
show ip sla auto endpoint-list	Displays configuration including default values of auto IP SLAs endpoint lists.

ip sla responder tcp-connect ipaddress

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for TCP Connect operations, use the **ip sla responder tcp-connect ipaddress** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

ip sla responder tcp-connect ipaddress *ip-address* **port** *port-number*

no ip sla responder tcp-connect ipaddress *ip-address* **port** *port-number*

Syntax Description

ip-address	Destination IP address.
port *port-number*	Specifies the destination port number.

Defaults

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor responder type tcpConnect ipaddress** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr responder type tcpConnect** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor responder type tcpConnect ipaddress** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor responder type tcpConnect ipaddress** command.

Usage Guidelines

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

Examples

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

```
ip sla responder tcp-connect ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla responder	Enables the IP SLAs Responder for nonspecific IP SLAs operations.

ip sla responder udp-echo ipaddress

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for User Datagram Protocol (UDP) echo or jitter operations, use the **ip sla responder udp-echo ipaddress** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

ip sla responder udp-echo ipaddress *ip-address* **port** *port-number*

no ip sla responder udp-echo ipaddress *ip-address* **port** *port-number*

Syntax Description

ip-address	Destination IP address.
port *port-number*	Specifies the destination port number.

Command Default

The IP SLAs Responder is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor responder type udpEcho ipaddress** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr responder type udpEcho** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor responder type udpEcho ipaddress** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor responder type udpEcho ipaddress** command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable UDP echo and jitter (UDP+) operations with control disabled.

Examples

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

```
ip sla responder udp-echo ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla responder	Enables the IP SLAs Responder for nonspecific IP SLAs operations.

ip sla restart

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

ip sla restart *operation-number*

Syntax Description

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

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor restart** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr restart** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor restart** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor restart** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

To restart an operation, the operation should be in an active state.

IP SLAs allows a maximum of 2000 operations.

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

Examples

The following example shows how to restart operation 12:

```
ip sla restart 12
```

Related Commands

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

ip sla schedule

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

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

no ip sla schedule *operation-number*

Syntax Description

operation-number	Number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts.
hh:*mm*[:*ss*]	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 *month* and *day.*
month	(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. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) 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.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after *hh*:*mm*:*ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
ageout *seconds*	(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
12.4(4)T	This command was introduced. This command replaces the **ip sla monitor schedule** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **rtr schedule** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **ip sla monitor schedule** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ip sla monitor schedule** command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.

Usage Guidelines

After you schedule the operation with the **ip sla schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the **ip sla** 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 **ip sla reaction-trigger** and **ip sla 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 **ip sla** 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 **ip sla 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.

The operation to can age out before it executes (that is, Z can occur before X). To ensure that this does not happen, configure the difference between the operation’s configuration time and start time (X and W) to 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 supported only for scheduling single IP SLAs operations. You cannot schedule multiple IP SLAs operations using the **ip sla 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.

The **ip sla schedule** command is supported in IPv4 networks. This command can also be used when configuring an IP SLAs operation that supports IPv6 addresses.

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 configuration in RAM).

```
ip sla 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:

```
ip sla schedule 1 start-time after 00:05:00
```

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

```
ip sla schedule 3 start-time now life forever
```

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

```
ip sla schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla group schedule	Performs group scheduling for IP SLAs operations.
ip sla reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLA.
ip sla 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 **ip sla reaction-configuration** global configuration command.
show ip sla configuration	Displays the configuration details of the IP SLAs operation.

life

To specify the lifetime characteristic in an auto IP Service Level Agreements (SLAs) scheduler, use the **life** command in IP SLA auto-measure schedule configuration mode. To return to the default, use the **no** form of this command.

life {**forever** | *seconds*}

no life

Syntax Description

forever	Runs operation indefinitely.
seconds	Length of time the operation actively collects information, in seconds (sec). Range is from 1 to 2147483647. Default is 3600.

Command Default

Auto IP SLAs operation actively collects information for 3600 sec.

Command Modes

IP SLA auto-measure schedule configuration (config-am-schedule)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the default configuration for life (3600 sec) in an auto IP SLA scheduler to the specified value.

Examples

The following example shows how to configure an auto IP SLAs scheduler that will cause an auto IP SLAs operation to actively collect data at 3:00 p.m. on April 5. The operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished its life. When the operation ages out, all configuration information for the operation is removed from the running configuration in RAM.

```
Router(config)#ip sla auto schedule apr5
Router(config-am-schedule)#ageout 43200
Router(config-am-schedule)#frequency 70
Router(config-am-schedule)#life 43200
Router(config-am-schedule)#probe-interval 1500
Router(config-am-schedule)#start-time 15:00 apr 5
Router(config-am-schedule)#end
Router#
Router# show ip sla auto schedule apr5
Group sched-id: apr5
    Probe Interval (ms) : 1500
    Group operation frequency (sec): 70
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: P15:00 apr 5
    Life (sec): 43200
    Entry Ageout (sec): 43200
Router#
```

Related Commands

Command	Description
react	Configures certain actions to occur based on events under the control of the auto P SLA scheduler.
show ip sla auto schedule	Displays the configuration including default values of an auto IP SLAs scheduler.

lives-of-history-kept

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **lives-of-history-kept** command is replaced by the **history lives-kept** command. See the **history lives-kept** command for more information.

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

lives-of-history-kept *lives*

no lives-of-history-kept

Syntax Description

lives	Number of lives maintained in the history table for the operation. If you specify 0 lives, history is not collected for the operation.

Defaults

0 lives

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **history lives-kept** command.
12.2(33)SRB	This command was replaced by the **history lives-kept** command.
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)SB	This command was replaced by the **history lives-kept** command.
12.2(33)SXI	This command was replaced by the **history lives-kept** command.

Usage Guidelines

The following rules apply to the **lives-of-history-kept** command:

- The number of lives you can specify is dependent on the type of operation you are configuring.
- The default value of 0 lives means that history is not collected for the operation.
- When the number of lives exceeds the specified value, the history table wraps (that is, the oldest information is replaced by newer information).
- When an operation makes a transition from a pending to active state, a life starts. When the life of an operation ends, the operation makes a transition from an active to pending state.

Note The **lives-of-history-kept** command does not support the IP SLAs User Datagram Protocol (UDP) jitter operation.

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.

To disable history collection, use the **no lives-of-history-kept** command rather than the **filter-for-history none** command. The **no lives-of-history-kept** command disables history collection before an IP SLAs operation is attempted. The **filter-for-history** command checks for history inclusion after the operation attempt is made.

Note 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.

Examples

The following example shows how to maintain the history for five lives of IP SLAs ICMP echo operation 1.

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 lives-of-history-kept 5
!
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 monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
samples-of-history-kept	Sets the number of entries kept in the history table per bucket for the IP SLAs operation.

lsp-selector

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

lsp-selector *ip-address*

no lsp-selector *ip-address*

Syntax Description

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

Command Default

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

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is used to force an IP SLAs operation to use a specific LSP to obtain its response time measurement. This option is useful if there are equal-cost multipaths between the source Provider Edge (PE) router and the Border Gateway Protocol (BGP) next hop neighbor.

You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source PE router. As specified in the example configuration, IP address 127.0.0.1 is the local host IP address chosen to select the LSP for obtaining response time measurements.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
```

```
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
 lsp-selector 127.0.0.1
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type
consecutive 3 action-type trapOnly
ip sla logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

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

lsp-selector-base

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

lsp-selector-base *ip-address*

no lsp-selector-base

Syntax Description

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

Command Default

The default base IP address is 127.0.0.0.

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

lsr-path

To define a loose source routing (LSR) path for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **lsr-path** command in the appropriate submode of IP SLA configuration or IP SLA configuration mode. To remove the definition, use the **no** form of this command.

lsr-path {*hostname1* | *ip-address1*} [[*hostname2* | *ip-address2*]...[*hostname8* | *ip-address8*]]

no lsr-path

Syntax Description

hostname1 | *ip-address1*	Destination hostname or IP address of the first hop in the LSR path.
[*hostname2* | *ip-address2*]...[*hostname8* | *ip-address8*]	(Optional) You can continue specifying host destinations until you specify the final host target. Each hostname or IP address specified indicates another hop on the path. The maximum number of hops you can specify is eight.

Defaults

LSR path is disabled.

Command Modes

IP SLA Configuration

ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)

IP SLA Monitor Configuration

ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)

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
12.0(3)T	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

The maximum number of hops available is eight when an LSR path is configured.

Note This command is supported by the IP SLAs Internet Control Message Protocol (ICMP) path echo and path jitter operations only.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see Table 16). 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 **lsr-path** command varies depending on the Cisco IOS release you are running (see Table 16) 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 **lsr-path** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

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

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T, 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, the LSR path is defined for IP SLAs ICMP path echo operation 1. The target destination for the operation is at 172.16.1.176. The first hop on the LSR path is 172.18.4.149. The second hop on the LSR path is 172.18.16.155. 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 16).

IP SLA Configuration

```
ip sla 1
 path-echo 172.16.1.176
 lsr-path 172.18.4.149 172.18.26.155
!
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
 lsr-path 172.18.4.149 172.18.26.155
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
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.

maximum-sessions

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

maximum-sessions *number*

no maximum-sessions

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

measurement-retry

To specify the number of times the endpoints belonging to an auto IP SLAs endpoint list are retested when an operation fails, use the **measurement-retry** command in IP SLAs endpoint-list auto-discovery configuration mode. To return to the default, use the **no** form of this command.

measurement-retry *number-of-retries*

no measurement-retry

Syntax Description

number-of-retries	Range is from 0 to 65535. Default is 0.

Command Default

No attempt to retry a failed operation is made.

Command Modes

IP SLA endpoint-list auto-discovery configuration (config-epl-disc)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command specifies the number of times an operation associated with an auto IP SLAs endpoint list is retried when a failure is detected.

This option is supported only by auto IP SLAs endpoint lists that are configured using auto discovery in Cisco IOS IP SLAs Engine 3.0.

Examples

The following example shows how to configure an auto IP SLAs endpoint lists of endpoints using auto discovery:

```
Router(config)#ip sla auto discover
Router(config)#ip sla auto endpoint-list type ip autolist
Router(config-epl)#discover port 5000
Router(config-epl)#measurement-retry 3
Router(config-epl)#access-list 3
Router(config-epl)#exit
Router# show ip sla auto endpoint-list
Endpoint-list Name: man1
    Description: testing manual build
    ip-address 10.1.1.1-7 port 23
    ip-address 10.1.1.9,10.1.1.15,10.1.1.23 port 23
Endpoint-list Name: autolist
    Description:
    Auto Discover Parameters
        Destination Port: 5000
        Access-list: 3
        Ageout: 3600    Measurement-retry: 3

    0 endpoints are discovered for autolist
```

Related Commands

Command	Description
show ip sla auto endpoint-list	Displays configuration including default values of auto IP SLAs endpoint lists.

mpls discovery vpn interval

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

mpls discovery vpn interval *seconds*

no mpls discovery vpn interval

Syntax Description

seconds	Specifies the time interval (in seconds) at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN. The default is 300.

Command Default

The default time interval is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When the BGP next hop neighbor discovery process is enabled (using the **mpls discovery vpn next-hop** command), a database of BGP next hop neighbors in use by any VPN routing or forwarding instance (VRF) associated with the source Provider Edge (PE) router is generated based on information from the local VRF and global routing tables. As routing updates are received, new BGP next hop neighbors are added immediately to the database. However, BGP next hop neighbors (that are no longer valid) are only removed from the database periodically as defined by the user (using the **mpls discovery vpn interval** command).

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

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 enable the MPLS VPN BGP next hop neighbor discovery process and specify 60 seconds as the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN:

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

Related Commands

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

mpls discovery vpn next-hop

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

mpls discovery vpn next-hop

no mpls discovery vpn next-hop

Syntax Description

This command has no arguments or keywords.

Command Default

The BGP next hop neighbor discovery process is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When the BGP next hop neighbor discovery process is enabled, a database of BGP next hop neighbors in use by any VPN routing or forwarding instance (VRF) associated with the source Provider Edge (PE) router is generated based on information from the local VRF and global routing tables. As routing updates are received, new BGP next hop neighbors are added immediately to the database. However, BGP next hop neighbors (that are no longer valid) are only removed from the database periodically as defined by the user (using the **mpls discovery vpn interval** command in global configuration mode).

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

Examples

The following example shows how to enable the MPLS VPN BGP next hop neighbor discovery process and specify 60 seconds as the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN:

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

Related Commands

Command	Description
mpls discovery vpn interval	Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
show mpls discovery vpn	Displays routing information relating to the MPLS VPN BGP next hop neighbor discovery process.

mpls lsp ping ipv4

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

mpls lsp ping ipv4 *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]

Syntax Description

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

Command Default

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

Command Modes

IP SLA configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type mpls lsp ping ipv4** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type mpls lsp ping ipv4** command.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

mpls lsp ping pseudowire

To configure an IP Service Level Agreements (SLAs) Multiprotocol Label Switching (MPLS) Pseudo-Wire Emulation Edge-to-Edge (PWE3) services via Virtual Circuit Connectivity Verification (VCCV) operation and enter VCCV configuration mode, use the **mpls lsp ping pseudowire** command in IP SLA configuration mode.

mpls lsp ping pseudowire *peer-ipaddr vc-id* [**source-ipaddr** *source-ipaddr*]

Syntax Description

peer-ipaddr	IPv4 address of the peer Provider Edge (PE) router.
vc-id	Virtual circuit (VC) identifier. The range is from 1 to 4294967295.
source-ipaddr *source-ipaddr*	(Optional) Specifies a source IP address for the originator of the pseudo-wire ping operation. When a source IP address is not specified, IP SLAs chooses the IP address nearest to the destination.

Command Default

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **mpls lsp ping pseudowire** command to configure a single IP SLAs VCCV operation, which checks MPLS label switched path (LSP) connectivity across an Any Transport over MPLS (AToM) VC by sending a series of pseudo-wire ping operations to the specified peer PE router. The IP SLA maintains pseudo-wire ping statistics for the operation, such as Round Trip Time (RTT). The optional **source-ipaddr** keyword is used to specify the *source-ipaddr* argument as the source IP address for the request originator.

To configure a faster measurement frequency (secondary frequency) to which an IP SLAs VCCV operation should change when a connection-loss or timeout condition occurs, use the **secondary-frequency** command in VCCV configuration mode.

To configure proactive threshold monitoring of an IP SLAs VCCV operation, configure actions to occur based on events under the control of that operation and enable Simple Network Management Protocol (SNMP) logging traps for that operation:

- To configure actions to occur based on events under the control of an IP SLAs operation, including the sending of SNMP logging trap when a specified violation type occurs for the monitored operation, use the **ip sla reaction-configuration** command in global configuration mode.
- To enable the generation of SNMP system logging messages specific to IP SLAs trap notifications, use the **ip sla logging traps** command in global configuration mode.

When these commands are used to configure continuous monitoring of PWE3 services, an IP SLAs VCCV operation can send out an SNMP trap if RTT threshold violations occur, if the connection is lost, or if a response times out.

To schedule an IP SLAs VCCV operation, use the **ip sla schedule** command in global configuration mode.

To display configuration values including all defaults for all IP SLAs operations or a specified operation, use the **show ip sla configuration** command. To display the current operational status and statistics for all IP SLAs operations or a specified operation, use the **show ip sla statistics** command. To display the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation, use the **show ip sla statistics aggregated** command. To display the reaction settings for all IP SLAs operations or a specified operation, use the **show ip sla reaction-configuration** command.

Examples

The following example shows how to manually configure operation parameters, reaction conditions, and scheduling options for IP SLAs VCCV operation 777.

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

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

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
ip sla reaction-configuration	Configures certain actions to occur based on events under the control of Cisco IOS IP SLAs.
ip sla schedule	Configures the scheduling parameters for a single IP SLAs operation.
secondary-frequency	Specifies a faster measurement frequency (secondary frequency) to which a Cisco IOS IP Service Level Agreements (SLAs) operation should change when a reaction condition occurs.

Command	Description
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.
show ip sla reaction-configuration	Displays the configured proactive threshold monitoring settings for all IP SLAs operations or a specified operation.
show ip sla statistics	Displays the current operational status and statistics for all IP SLAs operations or a specified operation
show ip sla statistics aggregated	Display the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operations.

mpls lsp trace ipv4

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

mpls lsp trace ipv4 *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]

Syntax Description

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

Command Default

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

Command Modes

IP SLA configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type mpls lsp trace ipv4** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type mpls lsp trace ipv4** command.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

num-packets

To specify the number of packets for a jitter operation in an auto IP Service Level Agreements (SLAs) operation template, use the **num-packets** command in the appropriate submode of the IP SLA template parameters configuration mode. To return to the default, use the **no** form of this command.

num-packets *packet-number*

no num-packets

Syntax Description

packet-number	Number of packets to be sent in each operation. Range is 1 to 60000. Default is 10 per operation.

Command Default

Default is 10 packets.

Command Modes

IP SLA Template Parameters Configuration

ICMP jitter configuration (config-icmp-jtr-params)
UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the number of packets sent during a jitter operation from the default (10) to the specified number of packets.

You must configure the type of IP SLAs operation, such as User Datagram Protocol (UDP) jitter or ICMP jitter, before you can configure any other parameters of the operation.

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

Examples

The following example shows how to configure an auto IP SLAs operation template for an ICMP jitter operation to change the number of packets from the default to 20 packets:

```
Router(config)#ip sla auto template type ip icmp-jitter 1
Router(config-tplt-icmp-jtr)#parameters
Router(config-icmp-jtr-params)#num-packets 20
Router(config-icmp-jtr-params)#end
Router# show ip sla auto template type ip icmp-jitter
IP SLAs Auto Template: 1
    Measure Type: icmp-jitter
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 20   Inter packet interval: 20
```

```
    Timeout: 5000          Threshold: 5000
Statistics Aggregation option:
    Hours of statistics kept: 2
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

Related Commands

Command	Description
ip sla auto template	Begins configuration for an IP SLAs operation template and enters IP SLA template configuration mode.
show ip sla auto template	Displays configuration including default values of an auto IP SLAs operation template.

operation-packet priority

To specify the packet priority in a Cisco IOS IP Service Level Agreements (SLAs) operation template, use the **operation-packet priority** command in the appropriate submode of IP SLA configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

operation-packet priority {**normal** | **high**}

no operation-packet priority

Syntax Description

normal	Specifies that the packet priority is normal. Default is normal.
high	Specifies that the packet priority is high.

Command Default

Packet priority is normal.

Command Modes

IP SLA Configuration

UDP jitter configuration (config-ip-sla-jitter)

IP SLA Template Parameters Configuration

UDP jitter configuration (config-udp-ech-params)

Command History

Release	Modification
12.4(6)T	This command was introduced. This command replaced the **probe-packet priority** command.
15.1(1)T	This command was modified. The UDP jitter submode of the IP SLA template parameters configuration mode was added.

Usage Guidelines

Increasing the packet priority of an IP SLAs operation can reduce the delay time for the packets in the queue.

This command is supported by the IP SLAs User Datagram Protocol (UDP) jitter operation only.

Before you can use this command to configure auto IP SLAs operation templates, you must enter the **parameters** command in IP SLA template configuration mode.

Examples

The following examples show how to enable microsecond precision, configure the Network Time Protocol (NTP) synchronization offset tolerance to 10 percent, and set the packet priority to high for an IP SLAs UDP jitter operation:

IP SLA Configuration

```
ip sla 1
 udp-jitter 205.199.199.2 dest-port 9006
```

```
 precision microseconds
 clock-tolerance ntp oneway percent 10
 operation-packet priority high
 frequency 300
!
ip sla schedule 1 life forever start-time after 00:00:06
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip udp-jitter 1
Router(config-udp-jtr-tplt)# parameters
Router(config-udp-jtr-params)# precision microseconds
Router(config-udp-jtr-params)# clock-tolerance ntp oneway percent 10
Router(config-udp-jtr-params)# operation-packet priority high
Router(config-udp-jtr-params)# end
Router#
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: 1
Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: usec       Operation packet priority: high
        NTP Sync Tolerance: 10 percent
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

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

owner

To configure the Simple Network Management Protocol (SNMP) owner of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **owner** command in the appropriate submode of IP SLA configuration, IP SLA auto Ethernet configuration, or IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

owner *text*

no owner

Syntax Description

text	Name of the SNMP owner from 0 to 255 ASCII characters.

Defaults

No owner is specified.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

IP SLA Auto Ethernet Configuration

Ethernet parameters configuration (config-ip-sla-ethernet-params)

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)

UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

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.
12.2(33)SRB	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
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 following configuration modes were added: • Ethernet echo • Ethernet jitter • Ethernet parameters • VCCV
12.4(20)T	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
12.2(33)SXI	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.

Usage Guidelines

The owner name contains one or more of the following: ASCII form of the network management station's transport address, network management station name (that is, the domain name), and network management personnel's name, location, or phone number. In some cases, the agent itself will be the owner of the operation. In these cases, the name can begin with "agent."

The **owner** 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 17). 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 **owner** command varies depending on the Cisco IOS release you are running (see Table 17) 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 **owner** command in ICMP echo configuration mode (config-sla-monitor-echo) within IP SLA monitor configuration mode.

Table 17 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

The following examples set the owner of IP SLAs ICMP echo operation 1 to 172.16.1.189 cwb.cisco.com User1 RTP 555-0100. 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 17).

IP SLA Configuration

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

```
ip sla 1
 icmp-echo 172.16.1.176
 owner 172.16.1.189 cwb.cisco.com User1 RTP 555-0100
!
ip sla schedule 1 life forever start-time now
```

IP SLA Monitor Configuration

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

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 owner 172.16.1.189 cwb.cisco.com User1 RTP 555-0100
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
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.

parameters

To enter IP SLA template parameters configuration mode and begin configuring operation-specific parameters in an auto IP Service Level Agreements (SLAs) operation template, use the **parameters** command in the appropriate submode of IP SLA template configuration mode. To return the configuration for all operation parameters to default values, use the no form of this command.

parameters

no parameters

Syntax Description

This command has no arguments or keywords.

Command Default

All operation parameters are configured with default values.

Command Modes

IP SLA Template Configuration

ICMP echo configuration (config-tplt-icmp-ech)
ICMP jitter configuration (config-tplt-icmp-jtr)
TCP connect configuration (config-tplt-tcp-conn)
UDP echo configuration (config-tplt-udp-ech)
UDP jitter configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enters IP SLA template parameters configuration mode for configuring operation-specific parameters in an auto IP SLAs operation template.

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

The commands available in IP SLA template parameters configuration mode differ depending on the operation being configured. Type **?** in IP SLA template-parameters configuration mode to see the operation-specific parameters that can be configured.

Examples

The following example shows how to modify certain operation-specific parameters in an auto IP SLAs operation template for a UDP jitter operation:

```
Router(config)# ip sla auto template type ip udp-jitter 1
Router(config-tplt-udp-jtr)# parameters
Router(config-udp-jtr-params)# precision microseconds
Router(config-udp-jtr-params)# clock-tolerance ntp oneway percent 10
Router(config-udp-jtr-params)# operation-packet high
Router(config-udp-jtr-params)# end
Router#
```

```
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: 1
Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: usec       Operation packet priority: high
        NTP Sync Tolerance: 10 percent
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

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

path-discover

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

path-discover

no path-discover

Syntax Description

This command has no arguments or keywords.

Command Default

The LSP discovery option is disabled.

Command Modes

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

Command History

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

Examples

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

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

Related Commands

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

path-echo

To configure a Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) path echo operation, use the **path-echo** command in IP SLA configuration mode.

path-echo {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type pathEcho protocol ipIcmpEcho** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type pathEcho protocol ipIcmpEcho** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type pathEcho protocol ipIcmpEcho** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type pathEcho protocol ipIcmpEcho** command.

Usage Guidelines

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

Examples

In the following example, IP SLAs operation 10 is configured as an ICMP path echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175:

```
ip sla 10
 path-echo 172.16.1.175
!
ip sla schedule 10 start-time now
```

Related Commands

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

path-jitter

To configure a Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) path jitter operation, use the **path-jitter** command in IP SLA configuration mode.

path-jitter {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
num-packets *packet-number*	(Optional) Specifies the number of packets to be transmitted in each operation. The default value is 10 packets per operation.
interval *milliseconds*	(Optional) Time interval between packets (in milliseconds). The default is 20.
targetOnly	(Optional) Sends test packets to the destination only (path is not traced).

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type pathJitter dest-ipaddr** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type pathJitter dest-ipaddr** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type pathJitter dest-ipaddr** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type pathJitter dest-ipaddr** command.

Usage Guidelines

If the **targetOnly** keyword is used, the ICMP path jitter operation will send echoes to the destination only (the path from the source to the destination is not traced).

If the **targetOnly** keyword is not used, the IP SLAs ICMP path jitter operation will trace a “hop-by-hop” IP path from the source to the destination and then send a user-specified number of test packets to each hop along the traced path at user-specified time intervals.

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

Examples

The following example show how to enable the ICMP path jitter operation to trace the IP path to the destination 172.69.5.6 and send 50 test packets to each hop with an interval of 30 ms between each test packet:

```
ip sla 2
 path-jitter 172.69.5.6 num-packets 50 interval 30
!
ip sla schedule 2 start-time now
```

Related Commands

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

paths-of-statistics-kept

To set the number of paths for which statistics are maintained per hour for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **paths-of-statistics-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.

paths-of-statistics-kept *size*

no paths-of-statistics-kept

Syntax Description

size	Number of paths for which statistics are maintained per hour. The default is 5.

Defaults

5 paths

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

A path is the route the request packet of the operation traverses through the network to get to its destination. The packet may take a different path to reach the same destination for each IP SLAs operation.

When the number of paths reaches the size specified, no further path-based information is stored.

Note This command is supported by the IP SLAs Internet Control Message Protocol (ICMP) path echo operation only.

For the IP SLAs ICMP path echo operation, the amount of router memory required to maintain the distribution statistics table is based on multiplying all of the values set by the following four commands:

- **distributions-of-statistics-kept**
- **hops-of-statistics-kept**
- **paths-of-statistics-kept**
- **hours-of-statistics-kept**

The general equation used to calculate the memory requirement to maintain the distribution statistics table for an ICMP path echo operation is as follows:
Memory allocation = (160 bytes) * (**distributions-of-statistics-kept** *size*) * (**hops-of-statistics-kept** *size*) * (**paths-of-statistics-kept** *size*) * (**hours-of-statistics-kept** *hours*)

Note To avoid significant impact on router memory, careful consideration should be used when configuring the **distributions-of-statistics-kept**, **hops-of-statistics-kept**, **paths-of-statistics-kept**, and **hours-of-statistics-kept** commands.

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 18). 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 **paths-of-statistics-kept** command varies depending on the Cisco IOS release you are running (see Table 18) 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 **paths-of-statistics-kept** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

Table 18 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

The following examples show how to maintain statistics for only three paths for IP SLAs ICMP path echo operation 2. 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 18).

IP SLA Configuration

```
ip sla 2
 path-echo 172.16.1.177
 paths-of-statistics-kept 3
!
ip sla schedule 2 life forever start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 2
 type pathEcho protocol ipIcmpEcho 172.16.1.177
 paths-of-statistics-kept 3
!
ip sla monitor schedule 2 life forever start-time now
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistics distributions kept per hop during the lifetime of the IP SLAs operation.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained 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.
statistics-distribution-interval	Sets the time interval for each statistics distribution kept for the IP SLAs operation.

precision

To set the level of precision at which the statistics for a Cisco IOS IP Service Level Agreements (SLAs) operation are measured, use the **precision** command in the UDP jitter submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

precision {**milliseconds** | **microseconds**}

no precision

Syntax Description

milliseconds	Sets the precision of IP SLAs operation measurements to 1 millisecond (ms). Milliseconds precision is configured by default.
microseconds	Sets the precision of IP SLAs operation measurements to 1 microsecond (usec).

Command Default

Measurements for the IP SLAs operation are displayed in milliseconds

Command Modes

IP SLA Configuration

UDP jitter configuration (config-ip-sla-jitter)

IP SLA Monitor Configuration

UDP jitter configuration (config-sla-monitor-jitter)

IP SLA Template Parameters Configuration

UDP jitter configuration (config-udp-jtr-params)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(1)T	This command was modified. The IP SLA template parameters configuration mode was added.

Usage Guidelines

This command changes value of the **precision** command from the default (milliseconds) to the specified value. If the **milliseconds** keyword is configured (default), the measurements for an IP SLAs operation will be displayed with the granularity of 1 ms. For example, a value of 22 equals 22 ms. If the **microseconds** keyword is configured, the measurements for an IP SLAs operation will be displayed with the granularity of 1 microsecond. For example, a value of 202 equals 202 microseconds.

This command is supported by the IP SLAs User Datagram Protocol (UDP) jitter operation only.

The **precision microseconds** command requires that both the source and IP SLAs Responder devices are running a version of Cisco IOS software that supports the **precision microseconds** command. See the "Command History" table for information about the supported Cisco IOS software releases.

Microsecond granularity for precision measurements is not supported on Cisco Catalyst 3000 and 2000 series switches that support IP SLAs. Do not configure the **microseconds** keyword with this command when you configure UDP jitter operations on devices running Cisco IOS Release 12.2SE and to which this limitation applies, such as Cisco Catalyst 3650 series switches. Use the Cisco Feature Navigator to find information about platform support for the Cisco IOS IP SLAs feature.

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

The configuration mode for the **precision** command varies depending on the Cisco IOS release you are running (see Table 19) and the operation type configured.

If you are using auto IP SLAs in Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **precision** command.

Table 19 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Examples

The following examples show how to enable microsecond precision, configure the Network Time Protocol (NTP) synchronization offset tolerance to 10 percent, and set the packet priority to high for an IP SLAs UDP jitter operation. 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 19).

IP SLA Configuration

```
ip sla 1
 udp-jitter 192.168.202.169 9006
 precision microseconds
 clock-tolerance ntp oneway percent 10
 probe-packet priority high
 frequency 300
!
ip sla schedule 1 life forever start-time after 00:00:06
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type jitter dest-ipaddr 192.168.202.169 dest-port 9006
 precision microseconds
 clock-tolerance ntp oneway percent 10
```

```
 probe-packet priority high
 frequency 300
!
ip sla monitor schedule 1 life forever start-time after 00:00:06
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip udp-jitter 1
Router(config-udp-jtr-tplt)# parameters
Router(config-udp-jtr-params)# precision microseconds
Router(config-udp-jtr-params)# clock-tolerance ntp oneway percent 10
Router(config-udp-jtr-params)# operation-packet high
Router(config-udp-jtr-params)# end
Router#
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: 1
Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: usec       Operation packet priority: high
        NTP Sync Tolerance: 10 percent
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

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

probe-interval

To configure the interval in an auto IP Service Level Agreements (SLAs) scheduler for staggering the start times of operations in Cisco IOS IP SLAs auto-measure groups that share the same schedule, use the **probe-interval** command in IP SLA auto-measure schedule configuration mode. To remove the interval configuration, use the **no** form of this command.

probe-interval *milliseconds*

no probe-interval

Syntax Description

milliseconds	Length of time, in milliseconds (ms). Range is from 100 to 99000. Default is 1000.

Command Default

There is a 1000 ms interval between the start time of one auto IP SLAs operation and the start time of the next auto IP SLAs operation being controlled by the same schedule.

Command Modes

IP SLAs auto-measure schedule configuration (config-am-schedule)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the default interval configuration (1000 ms) in an auto IP SLAs scheduler to the specified value.

An operation is created for each destination in an auto IP SLAs endpoint list specified for an IP SLAs auto-measure group.

Once the operations start, they continue operating based on the frequency specified by the **frequency** command.

Examples

The following example shows how to configure an auto IP SLAs scheduler that will cause an auto IP SLAs operation to actively collect data at 3:00 p.m. on April 5. The operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished its life. When the operation ages out, all configuration information for the operation is removed from the running configuration in RAM:

```
Router(config)#ip sla auto schedule apr5
Router(config-am-schedule)#ageout 43200
Router(config-am-schedule)#frequency 70
Router(config-am-schedule)#life 43200
Router(config-am-schedule)#probe-interval 1500
Router(config-am-schedule)#start-time 15:00 apr 5
Router(config-am-schedule)#end
Router#
Router# show ip sla auto schedule apr5
Group sched-id: apr5
    Probe Interval (ms) : 1500
```

```
    Group operation frequency (sec): 70
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: P15:00 apr 5
    Life (sec): 43200
    Entry Ageout (sec): 43200
Router#
```

Related Commands

Command	Description
frequency	Sets the frequency characteristic in an auto IP SLAs scheduler for restarting auto IP SLAs operations.
show ip sla auto schedule	Displays configuration including default values of auto IP SLAs schedulers.

probe-packet priority

Note Effective with Cisco IOS Release 12.4(6)T, the **probe-packet priority** command is replaced by the operation-packet-priority command. See the **operation-packet priority** command for more information.

To specify the packet priority of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **probe-packet priority** 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.

probe-packet priority {**normal** | **high**}

no probe-packet priority

Syntax Description

probe-packet priority normal	Sets the packet priority to normal. Packet priority is normal by default.
probe-packet priority high	Sets the packet priority to high.

Command Default

Packet priority is normal.

Command Modes

IP SLA Configuration

UDP jitter configuration (config-ip-sla-jitter)

IP SLA Monitor Configuration

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
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4(6)T	This command was replaced by the **operation-packet prority** command.

Usage Guidelines

Increasing the packet priority of an IP SLAs operation can reduce the delay time for the packets in the queue.

Note This command is supported by the IP SLAs User Datagram Protocol (UDP) jitter operation only.

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 19). 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 **probe-packet priority** command varies depending on the Cisco IOS release you are running (see Table 19) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the UDP jitter operation type is configured, you would enter the **probe-packet priority** command in UDP jitter configuration mode (config-sla-monitor-jitter) within IP SLA monitor configuration mode.

Table 20 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

Examples

The following examples show how to enable microsecond precision, configure the Network-Time Protocol (NTP) synchronization offset tolerance to 10 percent, and set the packet priority to high for IP SLAs UDP jitter 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 19).

IP SLA Configuration

```
ip sla 1
 udp-jitter 205.199.199.2 dest-port 9006
 precision microseconds
 clock-tolerance ntp oneway percent 10
 probe-packet priority high
 frequency 300
!
ip sla schedule 1 life forever start-time after 00:00:06
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type jitter dest-ipaddr 205.199.199.2 dest-port 9006
 precision microseconds
 clock-tolerance ntp oneway percent 10
 probe-packet priority high
 frequency 300
!
ip sla monitor schedule 1 life forever start-time after 00:00:06
```

Related Commands

Command	Description
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.

react (tplt-icmp-ech)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an Internet Control Message Protocol (ICMP) echo operation, use the **react** command in the ICMP echo submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** {*type-of-action*}] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **timeout**—Reaction should occur if there is a one-way timeout. • **verifyError**—Reaction should occur if there is a one-way error verification violation • **rtt**—Reaction should occur if round-trip time violates upper or lower threshold.
action-type	(Optional) Specifies action to be taken when threshold violations occur.
type-of-action	(Optional) Keywords for *type-of-action* are: • **none**—No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly**—A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-type never** keywords are configured, the **action-type** *type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upper threshold* or drops below the *lower threshold*.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* for **threshold-type average** is 3 and the upper threshold is 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 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.

threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If these keywords are configured, the **action-type none** and **action-type trapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when violation threshold for the monitored element is met x number of times within the last y number of measurements.
x-value y-value	(Optional) Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	Value in milliseconds. For defaults, see Table 21.
lower-threshold	Value in milliseconds. For defaults, see Table 21.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

ICMP echo submode of IP SLA template configuration (config-tplt-icmp-ech)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no form of** this command with one or more keywords can be used to disable individual monitored elements or use the **no react** command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Table 21 lists the default upper and lower thresholds for specific monitored elements.

Table 21 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
rtt	5000 ms	3000 ms

Only SNMP traps are supported for round-trip time (RTT) violations during non-Jitter operations.

Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.

Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

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

To display the current threshold monitoring configuration for an auto IP SLAs operation, use the **show ip sla auto template** command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the ICMP echo operation specifies that when three consecutive timeout events occur, an SNMP trap notification should be sent.

```
Router(config)#ip sla auto template type ip icmp-echo react-to
Router(config-tplt-icmp-ech)#react timeout action-type traponly threshold-type conecutive
3
Router(config-tplt-icmp-ech)#end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: react-to
    Measure Type: icmp-echo
    Description:
    .
    .
    .
    Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-icmp-jtr)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an Internet Control Message Protocol (ICMP) jitter operation, use the **react** command in the ICMP jitter submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** {*type-of-action*}] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **jitterAvg**—Reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg**—Reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg**—Reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold. • **latencyDSAvg**—Reaction should occur if the average one-way destination-to-source latency value violates the upper threshold or lower threshold. • **latencySDAvg**—Reaction should occur if the average one-way source-to-destination latency value violates the upper threshold or lower threshold. • **maxOfLatencyDS**—Reaction should occur if the one-way maximum destination-to-source latency value is violated. • **maxOfLatencySD**—Reaction should occur if the one-way maximum source-to-destination latency value is violated. • **maxOfNegativeDS**—Reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD**—Reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated. • **maxOfPositiveDS**—Reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD**—Reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated.

monitored-element (continued)	• **packetLateArrival**—Reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLoss**—Reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is either destination-to-source or source-to-destination. • **packetOutOfSequence**—Reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt**—Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **successivePacketLoss** • **timeout**—Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError**—Reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Keywords for *type-of-action* are: • **none**—No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly**—A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-type never** keywords are configured, the **action-type** *type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upper threshold* or drops below the *lower threshold*.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-type average** is 3 and the upper threshold is 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 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.

threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If these keywords are configured, the **action-type none** and **action-type trapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	(Optional) Value in milliseconds (ms). For defaults, see Table 23.
lower-threshold	(Optional) Value in milliseconds (ms). For defaults, see Table 23.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

ICMP jitter submode of IP SLA template configuration (config-tplt-icmp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no** form of this command with one or more keywords can be used to disable individual monitored elements or use the **no** form of this command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Return-trip time (RTT) reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).

SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation.

For Mean opinion score (MOS), values are computed as numbers to two decimal places, from a value of 1.00 (worst quality) to 5.00 (best quality). The number for *upper-threshold* and *lower-threshold* is expressed in three 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).

Table 23 lists the default upper and lower thresholds for specific monitored elements.

Table 22 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms
jitterSDAvg	100 ms	100 ms
latencyDSAvg	5000 ms	3000 ms
latencySDAvg	5000 ms	3000 ms
maxOflatencyDS	5000 ms	3000 ms
maxOflatencySD	5000 ms	3000 ms
maxOfNegativeDS	10000 ms	10000 ms
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
mos	500 (score)	100 (score)
packetLateArrival	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rtt	5000 ms	3000 ms

Only syslog messages are supported for RTTAvg threshold violations.

Only syslog messages are supported for RTT violations during Jitter operations.

Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.

Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB.

Use the **snmp-server enable traps rtr** or **snmp-server enable traps syslog** command to enable the sending of IP SLAs SNMP trap notifications.

Use the **ip sla logging traps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Only system logging messages are supported for RTTAvg threshold violations.

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **show ip sla auto template** command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the ICMP jitter operation specifies that when three consecutive packet loss events occur, an SNMP trap notification should be sent:

```
Router(config)#ip sla auto template type ip icmp-jitter react-closs
Router(config-tplt-icmp-jtr)#react packetloss action-type traponly threshold-type
conecutive 3
Router(config-tplt-icmp-jtr)#end
Router# show ip sla auto template type ip icmp-jitter
IIP SLAs Auto Template: react
    Measure Type: icmp-jitter
    .
    .
    .
    Reaction Configuration:
        Reaction Index       : 1
          Reaction           : packetLoss
          Threshold Type     : Consecutive
          Threshold Rising   : 3
          Threshold Falling  : 10000
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto for IP SLAs a operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-tcp-conn)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an Transmission Control Protocol (TCP) connect operation, use the **react** command in the TCP connect submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** {*type-of-action*}] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **connectionLoss**—Reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **rtt**—Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **timeout**—Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Keywords for *type-of-action* are: • **none**—No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly**—A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-type never** keywords are configured, the **action-type** *type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upper threshold* value or drops below the *lower threshold* value.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-type average** is 3 and the upper threshold is 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 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.

occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Threshold violations should not be monitored. This is the default threshold type. **Note** If the **threshold-type never** keywords are configured, the **action-type none** and **action-type trapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	(Optional) Value in milliseconds (ms). For defaults, see Table 23.
lower-threshold	(Optional) Value in milliseconds (ms). For defaults, see Table 23.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

TCP connect submode of IP SLA template configuration (config-tplt-tcp-conn)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no** form of this command with one or more keywords can be used to disable individual monitored elements or use the **no** form of this command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Table 23 lists the default upper and lower thresholds for specific monitored elements.

Table 23 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
rtt	5000 ms	3000 ms

Only SNMP traps are supported for return-trip time (RTT) violations during non-Jitter operations.

Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.

Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

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

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **show ip sla auto template** command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the TCP connect operation specifies that when three timeout connection loss events occur, an SNMP trap notification should be sent:

```
Router(config)#ip sla auto template type ip tcp-connect react-to
Router(config-tplt-tcp-conn)#react timout action-type traponly threshold-type conecutive 3
Router(config-tplt-tcp-conn)#end
Router# show ip sla auto template type ip tcp-connect
IP SLAs Auto Template: react-to
    Measure Type: tcp-connect
    Description:
    .
    .
    .
    Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-udp-ech)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for a User Datagram Protocol (UDP) echo operation, use the **react** command in the UDP echo submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** {*type-of-action*}] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **connectionLoss**—Reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **rtt**—Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **timeout**—Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError**—Reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Valid keywords are: • **none**—No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly**—A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-type never** keywords are configured, the **action-type** *type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upper threshold* or drops below the *lower threshold*.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-type average** is 3 and the upper threshold is 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 ms and the average exceeds the upper threshold of 5000 ms.

threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If the **threshold-type never** keywords are configured, the **action-type none** and **action-type trapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	(Optional) Value in milliseconds (ms). For defaults, see Table 23.
lower-threshold	(Optional) Value in milliseconds (ms). For defaults, see Table 23.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

UDP echo submode of IP SLA template configuration (config-tplt-udp-ech)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times to allow reactions for multiple monitored elements.

The **no** form of this command with one or more keywords can be used to disable individual monitored elements or use the **no** form of this command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Table 23 lists the default upper and lower thresholds for specific monitored elements.

Table 24 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
rtt	5000 ms	3000 ms

Only SNMP traps are supported for round-trip time (RTT) violations during non-Jitter operations.

Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.

Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

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

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **show ip sla auto template** command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the UDP echo operation specifies that when three consecutive timeout events occur, an SNMP trap notification is sent:

```
Router(config)#ip sla auto template type ip udp-echo react-to
Router(config-tplt-udp-ech)#react timeout action-type traponly threshold-type conecutive 3
Router(config-tplt-udp-ech)#end
Router# show ip sla auto template type ip udp-echo
IP SLAs Auto Template: react-to
    Measure Type: udp-echo
    Description:
    .
    .
    .
    Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-udp-jtr)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an User Datagram Protocol (UDP) jitter operation, use the **react** command in the UDP jitter submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** *type-of-action*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **connectionLoss**—Reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **icpif**—Calculated Planning Impairment Factor. • **jitterAvg**—Reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg**—Reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg**—Reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold. • **latencyDSAvg**—Reaction should occur if the average one-way destination-to-source latency value violates the upper threshold or lower threshold. • **latencySDAvg**—Reaction should occur if the average one-way source-to-destination latency value violates the upper threshold or lower threshold. • **maxOfLatencyDS**—Reaction should occur if the one-way maximum destination-to-source latency value is violated. • **maxOfLatencySD**—Reaction should occur if the one-way maximum source-to-destination latency value is violated. • **maxOfNegativeDS**—Reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD**—Reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated. • **maxOfPositiveDS**—Reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD**—Reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated.

monitored-element (continued)	• **mos—**Mean Opinion Score (mos) in either direction rises above or falls below a specified threshold. • **packetLateArrival**—Reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLossDS**—Reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetLossSD**—Reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetMIA**—Reaction should occur if the packet is not returned. • **packetOutOfSequence**—Reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt**—Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **timeout**—Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError**—Reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Valid keywords are: • **none**—No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly**—A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-type never** keywords are configured, the **action-type** *type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upper threshold* or drops below the *lower threshold*.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-type average** is 3 and the upper threshold is 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 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.

threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If these keywords are configured, the **action-type none** and **action-type trapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	(Optional) Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	Value in milliseconds (ms). For defaults, see Table 23.
lower-threshold	Value in milliseconds (ms). For defaults, see Table 23.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

UDP jitter submode of IP SLA template configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no** form of this command with one or more keywords can be used to disable individual monitored elements or use the **no react** command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Return-trip time (RTT) reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).

SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation.

For Mean opinion score (MOS), values are computed as numbers to two decimal places, from a value of 1.00 (worst quality) to 5.00 (best quality). The numbers for *upper-threshold* and *lower-threshold* arguments are expressed in three 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).

Table 23 lists the default upper and lower thresholds for specific monitored elements.

Table 25 Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms
jitterSDAvg	100 ms	100 ms
latencyDSAvg	5000 ms	3000 ms
latencySDAvg	5000 ms	3000 ms
maxOflatencyDS	5000 ms	3000 ms
maxOflatencySD	5000 ms	3000 ms
maxOfNegativeDS	10000 ms	10000 ms
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
mos	500 (score)	100 (score)
packetLateArrival	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rtt	5000 ms	3000 ms

Only syslog messages are supported for RTTAvg threshold violations.

Only syslog messages are supported for RTT violations during Jitter operations.

Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.

Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB.

Use the **snmp-server enable traps rtr** or **snmp-server enable traps syslog** command to enable the sending of IP SLAs SNMP trap notifications.

Use the **ip sla logging traps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Only system logging messages are supported for RTTAvg threshold violations.

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **show ip sla auto template** command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the UDP jitter operation specifies that when three consecutive timeout events occur, an SNMP trap notification should be sent:

```
Router(config)#ip sla auto template type ip udp-jitter react-to
Router(config-tplt-udp-jtr)#react timeout action-type traponly threshold-type conecutive 3
Router(config-tplt-udp-jtr)#end
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: react-to
    Measure Type: udp-jitter
    Description:
    .
    .
    .
    Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

reply-dscp-bits

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

reply-dscp-bits *dscp-value*

no reply-dscp-bits *dscp-value*

Syntax Description

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

Command Default

The DSCP value is 0.

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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, IP SLA monitor configuration, or IP SLA template parameters 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

bytes	Size of the protocol data in the payload of the request packet of the operation, in bytes. Range is from 0 to the maximum supported by the protocol.

Command Default

The default data size varies 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)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-icmp-ech-params)

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.
15.1(1)T	This command was modified. The IP SLA template-parameters configuration mode was added.

Usage Guidelines

The **request-data-size** command can be 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 to configure 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 26). If you are configuring an IP SLAs label switched path (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 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.

If you are running Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **request-data size** command.

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, 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 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Examples

The following examples show how to set the request packet size to 40 bytes for an IP SLAs ICMP echo operation. 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 26).

IP SLA Configuration

```
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

```
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
```

IP SLA Template Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-icmp-ech-tplt)# parameters
Router(config-icmp-ech-params)# request-data-size 40
Router(config-icmp-ech-params)# end
Router#
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: 1
Measure Type: icmp-echo (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 40 Verify Data: false
       Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

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 auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template 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

bytes	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

operation-number	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

group-operation-number	Group configuration or group schedule number of the IP SLAs operation to be scheduled. The range is from from 0 to 65535.
operation-id-numbers	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: • 2, 3, 4, 9, 20 • 10-20, 30-35, 60-70 • 2, 3, 4, 90-100, 105-115 The *operation-id-numbers* argument can include a maximum of 125 characters.
schedule-period *schedule-period-range*	Time (in seconds) for which the IP SLAs operation group is scheduled. The range is from 1 to 604800.
ageout *seconds*	(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 *group-operation-frequency*	(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 *seconds*	(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**.
hh:*mm*[:*ss*]	(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 *month* and *day*.
month	(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.
day	(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 *hh*:*mm*:*ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* 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

name	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

value	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

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

Command Default

No LSP Health Monitor operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(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.

```
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

operation-number	Number of the LSP Health Monitor operation for which reactions are to be configured.
react *monitored-element*	Specifies the element to be monitored for violations. Keyword options for the monitored element are: • **connectionLoss**—Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. • **timeout**—Specifies that a reaction should occur if there is a one-way timeout for the monitored operation.
action-type *option*	(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 *option* argument can be one of the following keywords: • **none**—No action is taken. This option is the default value. • **trapOnly**—Send an SNMP logging trap when the specified violation type occurs for the monitored element.
threshold-type consecutive [*occurrences*]	(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 *occurrences* 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

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

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
12.2(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

operation-number	Number of the IP SLAs operation to configure for which reactions are to be configured.
react *monitored-element*	Specifies the element to be monitored for threshold violations. Keyword options for the *monitored-element* are: **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. **jitterAvg**—Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. **jitterDSAvg**—Specifies that a reaction should occur if the average destination-to-source (DS) jitter value violates the upper threshold or lower threshold. **jitterSDAvg**—Specifies that a reaction should occur if the average source-to-destination (SD) jitter value violates the upper threshold or lower threshold. **mos**—Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold.

react *monitored-element* (continued)	**PacketLossDS**—Specifies that a reaction should occur if the destination-to-source packet loss value violates the upper threshold or lower threshold. **PacketLossSD**—Specifies that a reaction should occur if the source-to-destination packet loss value violates the upper threshold or lower threshold. **rtt**—Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold. **timeout**—Specifies that a reaction should occur if there is a timeout for the monitored operation. Thresholds do not apply to this monitored element. **verifyError**—Specifies that a reaction should occur if there is an error verification violation. Thresholds do not apply to this monitored element.
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 [*consecutive-occurences*]	When a threshold violation is met for the monitored element five times in a row, perform the action defined by **action-type**. The optional *consecutive-occurences* argument can be used to change the number of consecutive occurences from the default of 5. The valid range is from 1 to 16. The *consecutive-occurences* value will appear in the output of the **show rtr reaction-configuration** command as the "Threshold Count:" value.
threshold-type xofy [*x-value y-value*]	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 *x-value* and *y-value* (**xofy 5 5**). The valid range for each value is from 1 to 16. The *x-value* value will appear in the output of the **show rtr reaction-configuration** command as the "Threshold Count:" value, and the *y-value* will appear as the "Threshold Count2:" value.
threshold-type average [*number-of-measurements*]	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. The default number of 5 averaged measurements can be changed using the optional *number-of-measurements* argument. The valid range from 1 to 16. 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.

[**threshold-value** *upper-threshold lower-threshold*]	(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 *option*	(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: • **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	This command was enhanced to provide new monitored elements and reaction options. The old syntax of **rtr reaction-configuration** *operation-number* [**verify-error-enable**] [**connection-loss-enable**] [**timeout-enable**] [**threshold-falling** *milliseconds*] [**threshold-type** *option*] [**action-type** *option*] was replaced by the syntax shown above. **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. • 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** *milliseconds* syntax (and the **threshold** RTR configuration command) was replaced by the **threshold-value** *upper-threshold lower-threshold* 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) of 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

operation-number	Number of the operation in the active state that has the **action-type** set with the **rtr reaction-configuration** global configuration command.
target-operation	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
```

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 *ip-address*	(Optional) Specifies the IP address that the operation will be received at.
port *port*	(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 *ip-address*	Specifies the IP address that the operation will be received at.
port *port*	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

operation-number	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

group-operation-number	Group configuration or group schedule number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	Time when the operation starts.
hh:*mm*[:*ss*]	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 *month* and *day*.
month	(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.
day	(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 *hh*:*mm*:*ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
ageout *seconds*	(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

samples	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 28). 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 28) 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 28 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 28).

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

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

Command Default

Scan interval is 240 minutes.

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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

minutes	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 rediscovery time period has not yet expired, then the next iteration of the LSP discovery process will not start until the time period has expired.

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

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

Examples

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

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

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

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

schedule

To add an auto IP Service Level Agreements (SLAs) scheduler to the configuration of an IP SLAs auto-measure group, use the **schedule** command in IP SLA auto-measure group configuration mode. To stop operations of the group, use the **no** form of this command.

schedule *schedule-id*

no schedule *schedule-id*

Syntax Description

schedule-id	ID of an already-configured auto IP SLAs scheduler.

Command Default

The operation in the group being configured is not scheduled.

Command Modes

IP SLA auto-measure group configuration (config-am-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command specifies an auto IP SLAs scheduler as a reference for the IP SLAs auto-measure group being configured.

Only one auto IP SLAs scheduler can be specified for each IP SLAs auto-measure group. Each scheduler can be referenced by more than one group.

To create a multioperation schedule, specify the same auto IP SLAs scheduler for two or more IP SLAs auto-measure groups.

You cannot modify the configuration of an auto-measure group if the specified auto IP SLAs scheduler has a start time other than Pending trigger (default). If you attempt to modify a group configuration that includes an active scheduler, the following message appears:

```
%Group is active, cannot make changes
```

To modify the configuration of an IP SLAs auto-measure group that includes an active auto IP SLAs scheduler with a specified start time, use the **no** form of this command to remove the scheduler from the group configuration, and then finish configuring the group before adding an active scheduler to the configuration. You can also configure the start time for a scheduler after adding the scheduler to the group configuration.

To create an auto IP SLAs scheduler, use the **ip sla auto schedule** command.

Examples

The following example shows how to add an auto IP SLAs scheduler to the configuration of an IP SLAs auto-measure group:

```
Router(config)#ip sla auto group type ip 1
Router(config-am-grp)#destination 1
```

```
Router(config-am-grp)#schedule 1
Router(config-am-grp)#end
Router#
Router# show ip sla auto group
Group Name: 1
    Description:
    Activation Trigger: Pending
    Destination: 1
    Schedule: 1

IP SLAs Auto Template: default
    Measure Type: icmp-jitter
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None

IP SLAs auto-generated operations of group 1
    no operation created
```

Related Commands

Command	Description
ip sla auto schedule	Begins configuration for an auto IP SLAs scheduler and enters IP SLA auto-measure schedule 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.
frequency	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-vccv)

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 29). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see Table 30 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 29 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 30 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

seconds	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.

show ip sla application

To display global information about Cisco IOS IP Service Level Agreements (SLAs), use the **show ip sla application** command in user EXEC or privileged EXEC mode.

show ip sla application

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor application** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr application** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor application** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor application** command.
12.4(22)T	This command was modified. The command output has been modified to include information on IP SLAs Event Publisher.
12.2(33)SRE	This command was modified. The command output has been modified to include information on IP SLAs Event Publisher and IP SLAs Ethernet operation measurements.

Usage Guidelines

Use the **show ip sla application** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show ip sla application** command:

```
Router# show ip sla application

IP Service Level Agreement Technologies

IPSLAs Infrastructure version: Engine-II

Supported Operation Types:
        802.1agEcho, 802.1agJitter, dhcp, dns, echo, frameRelay, ftp
        http, icmpJitter, jitter, lspGroup, lspPing, lspTrace
        pathEcho, pathJitter, rtp, tcpConnect, udpEcho, voip
Supported Features:
IPSLAs Event Publisher
IP SLAs low memory water mark: 0

Estimated system max number of entries: 63840
Estimated number of configurable operations: 63840
Number of Entries configured  : 0
```

```
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0

Last time the operation configuration changed: *07:22:13.183 UTC Fri Feb 13 2009


Router#
```

Table 1 describes the significant fields shown in the display.

Table 31 show ip sla application Field Descriptions

Field	Description
IPSLAs Infrastructure version	The version of the IPSLAs infrastructure supported on the router.
Supported Operation Types	The types of operations supported by the command.
Supported Features	The features supported by the command.

Related Commands

Command	Description
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla authentication

To display Cisco IOS IP Service Level Agreements (SLAs) authentication information, use the **show ip sla authentication** command in user EXEC or privileged EXEC mode.

show ip sla authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor authentication** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr authentication** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor authentication** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor authentication** command.

Usage Guidelines

Use the **show ip sla authentication** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show ip sla authentication** command:

```
Router# show ip sla authentication

IP SLA Monitor control message uses MD5 authentication, key chain name is: ipsla
```

Related Commands

Command	Description
show ip sla configuration	Displays configuration values for IP SLAs operations.

show ip sla auto discovery

To display the status of IP Service Level Agreements (SLAs) auto discovery and the configuration of auto IP SLAs endpoint lists configured to use auto discovery, use the **show ip sla auto discovery** command in user EXEC or privileged EXEC mode.

show ip sla auto discovery

Syntax Description

This command has no arguments or keywords.

Command Default

Displays the configuration of IP SLAs auto discovery.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following is sample output from the **show ip sla auto discovery** command before, and after, auto discovery was enabled. Note that no IP SLAs endpoint lists are configured yet.

```
Router>show ip sla auto discovery
IP SLAs auto-discovery status: Disabled

The following Endpoint-list are configured to auto-discovery:

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip sla auto discovery
Router(config)#exit
Router#
Router# show ip sla auto discovery
IP SLAs auto-discovery status: Enabled

The following Endpoint-list are configured to auto-discovery:
```

Table 32 describes the significant fields shown in the display.

Table 32 **show ip sla auto discovery *Field Descriptions***

Field	Description
IP SLAs auto-discovery status	Configuration of the **ip sla auto discovery** command.

Related Commands

Command	Description
ip sla auto discovery	Enables IP SLAs auto discovery in Cisco IP SLAs Engine 3.0.

show ip sla auto endpoint-list

To display the configuration including default values of all auto IP Service Level Agreements (SLAs) endpoint lists, all auto IP SLAs endpoint lists for a specified operation type, or a specified auto IP SLAs endpoint list, use the **show ip sla auto endpoint-list** command in user EXEC or privileged EXEC mode.

show ip sla auto endpoint-list [**type ip** [*template-name*]]

Syntax Description

type ip	(Optional) Specifies that the operation type is Internet Protocol.
template-name	(Optional) Unique identifier of the endpoint list. String of 1 to 64 alphanumeric characters.

Command Default

Default display includes configuration for all auto IP SLAs endpoint lists.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following is sample output from the **show ip sla auto endpoint-list** command for all configured endpoint lists. Because all of the destinations are for IP operations, the **type ip** keyword is not configured.

```
Router# show ip sla auto endpoint-list
Endpoint-list Name: man1
    Description: testing manual build
    ip-address 10.1.1.1-7 port 23
    ip-address 10.1.1.9,10.1.1.15,10.1.1.23 port 23

Endpoint-list Name: autolist
    Description:
    Auto Discover Parameters
        Destination Port: 5000
        Access-list: 3
        Ageout: 3600    Measurement-retry: 3

    0 endpoints are discovered for autolist
```

Table 32 describes the significant fields shown in the display.

Table 33 **show ip sla auto endpoint-list *Field Descriptions***

Field	Description
Destination Port	Port number of target device or Cisco IP SLAs Responder.
Access-list	Name of list of discovered endpoints.

Field	Description
Ageout	Length of time that operation is kept in memory, in seconds (sec).
Measurement-retry	Number of times the endpoints belonging to an auto IP SLAs destination templates are retested when an operation fails.

Related Commands

Command	Description
access-list (epl-disc)	Adds list of discovered endpoints to an auto IP SLAs endpoint list.
ageout	Adds ageout timer to auto IP SLAs scheduler or endpoint list.
ip sla auto endpoint-list	Enters IP SLA endpoint-list configuration mode and begins creating an auto IP SLAs endpoint list.
measurement-retry	Specifies the number of times an operation associated with an auto IP SLAs endpoint list is retried when a failure is detected.

show ip sla auto group

To display configuration values including all defaults for all Cisco IOS IP Service Level Agreements (SLAs) auto-measure groups or a specified group, use the **show ip sla auto group** command in user EXEC or privileged EXEC mode.

show ip sla auto group [**type ip** [*group-name*]]

Syntax Description

type ip	(Optional) Specifies that the operation type is Internet Protocol.
group-name	(Optional) Unique identifier of auto-measure group. String of 1 to 64 alphanumeric characters.

Command Default

Displays configuration for all IP SLAs endpoint lists.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command displays the configuration of an IP SLAs auto-measure group including all default values and information about operations created for each destination in the specified endpoint-list for this group.

Examples

The following is sample output from the **show ip sla auto group** command for an IP SLAs auto-measure group (test) and the created operations within the group:

```
Router# show ip sla auto group test
Group Name: test
    Description:
    Activation Trigger: Immediate
    Destination: testeplist
    Schedule: testsched
    Measure Template: testtplt(icmp-jitter)
IP SLAs auto-generated operations of group test

  sno     oper-id         type             dest-ip-addr/port
    1   299389922      icmp-jitter           20.1.1.32/NA
```

Table 32 describes the significant fields shown in the display.

Table 34 **show ip sla auto group *Field Descriptions***

Field	Description
Activation Trigger	Start time of operation.
Destination	Name of auto IP SLAs endpoint list referenced by the auto-measure group.
Schedule	Name of auto IP SLAs scheduler referenced by the auto-measure group.
Measure Template	Name of auto IP SLAs template referenced by the auto-measure group.
sno	Serial number of IP SLAs operation created for specified endpoint.
oper-id	Entry number of IP SLAs operation created for specified endpoint.
type	Type of IP SLAs operation created for specified endpoint.
dest-ip-addr/port	IP address and port of destination for operation in current display.

Related Commands

Command	Description
ip sla auto group	Begins configuration for an IP SLAs auto-measure group and enters IP SLA auto-measure group configuration mode.

show ip sla auto schedule

To display configuration values including all defaults for all auto IP Service Level Agreements (SLAs) schedulers or a specified scheduler, use the **show ip sla auto template** command in user EXEC or privileged EXEC mode.

show ip sla auto schedule [*schedule-id*]

Syntax Description

schedule-id	(Optional) Unique identifier for IP SLAs schedule. String of 1 to 64 alphanumeric characters.

Command Default

The default output includes the configuration for all auto IP SLAs schedulers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following is sample output from the **show ip sla auto schedule** command when you specify an auto IP SLAs scheduler by name (basic-default):

```
Router# show ip sla auto schedule basic-default
Group sched-id: basic-default
    Probe Interval (ms): 1000
    Group operation frequency (sec): 60
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: Pending trigger
    Life (sec): 3600
    Entry Ageout (sec): never
```

Table 32 describes the significant fields shown in the display.

Table 35 **show ip sla auto schedule *Field Descriptions***

Field	Description
Probe Interval (ms)	Length of time, in milliseconds (ms), between operations that share the same auto IP SLAs scheduler.
Group operation frequency (sec)	Frequency at which each operation repeats, in seconds (sec).
Next Scheduled Start Time	Start time of operation. “Pending trigger” indicates that neither a specific start time nor a reaction trigger is configured.
Life (sec)	Length of time that the operation runs, in seconds (sec).
Entry Ageout (sec)	Length of time that operation is kept in memory, in seconds (sec).

Related Commands

Command	Description
ageout (IP SLA)	Adds ageout timer to auto IP SLAs scheduler or endpoint list.
frequency	Specifies how often an operation in an IP SLAs auto-measure group will repeat once it is started.
ip sla auto schedule	Enters IP SLA auto-measure schedule configuration mode and begins creating an auto IP SLAs scheduler.
life	Specifies lifetime characteristic in an auto IP SLAs scheduler.
probe-interval	Specifies interval between operations for staggering operations that share the same auto IP SLAs scheduler.
react	Configures reaction and proactive threshold monitoring parameters in an auto IP SLAs operation template.
start-time	Specifies start time for an IP SLAs auto-measure group.

show ip sla auto summary-statistics

To display the current operational status and statistics for a Cisco IOS IP Service Level Agreements (SLAs) auto-measure group or for a specified destination of a group, use the **show ip sla auto summary-statistics** command in user EXEC or privileged EXEC mode.

show ip sla auto summary-statistics group type ip *group-name* [**ip-address** *ip-address* [**port** *port*]]

Syntax Description

group-name	Unique identifier for IP SLAs auto-measure group. String of 1 to 64 alphanumeric characters.
ip-address *ip-address*	(Optional) Specifies IPv4 address of destination routing device or destination Cisco IP SLAs Responder.
port *port*	(Optional) Specifies port number of destination routing device or destination Cisco IP SLAs Responder. Range is from 1 to 65535.

Command Default

The default output includes statistics for all endpoints of the operation in an IP SLA auto-measure group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following is sample output from the **show ip sla auto summary-statistics** for an IP SLAs auto-measure group (test) that started immediately upon configuration. The partial output from the **show running-config** and **show ip sla group** command are included to illustrate the relationship between the group, operation, and scheduler. Notice that the command to start the operations was configured after the auto IP SLAs scheduler (testsched) was added to the group configuration.

```
Router# show running-config
.
.
.
ip sla auto template type ip icmp-jitter test
ip sla auto endpoint-list type ip test
  ip-address 10.1.1.32 port 2222
ip sla auto group type ip test
schedule testsched
template icmp-jitter testtplt
destination testeplist
ip sla auto schedule testsched <<=====
  start-time now
.
.
.
Router# show ip sla auto summary-statistics group type ip icmp-jitter test
```

```
IP SLAs Auto Group Summary Statistics

Legend -
  sno: Serial Number in current display
  oper-id: Entry Number of IPSLAs operation
  type: Type of IPSLAs operation
  n-rtts: Number of successful round trips in current hour
          of operation
  rtt (min/av/max): The min, max and avg values of latency in
                    current hour of operation
  avg-jitter(DS/SD): average jitter value in destination to
                     source and source to destination direction
  pak-loss: accumulated sum of source to destination and
            destination to source packet loss in current hour

Summary Statistics:
Auto Group Name: test
Template: testtplt

Number of Operations: 1
  sno    oper-id    type      n-rtts    rtt       avg-jitter    packet
                                (min/avg/max)      (DS/SD)       loss
   1    299389922  icmp-jitter  10     8/16/24 ms         9/0 ms        0

Router# show ip sla auto group
Group Name: test
    Description:
    Activation Trigger: Immediate
    Destination: testeplist
    Schedule: testsched
    Measure Template: testtplt(icmp-jitter)
IP SLAs auto-generated operations of group test

  sno     oper-id         type             dest-ip-addr/port
    1   299389922      icmp-jitter           10.1.1.32/NA
```

Related Commands

Command	Description
ip sla auto group	Begins configuration for an IP SLAs auto-measure group and enters IP SLA auto-measure group configuration mode.
ip sla auto endpoint-list	Begins configuration for an auto IP SLAs endpoint-list and enters IP SLA endpoint-list configuration mode.
ip sla auto schedule	Begins configuration for an auto IP SLAs scheduler and enters IP SLA auto-measure schedule configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.

show ip sla auto template

To display configuration values including all defaults for all Cisco IOS IP Service Level Agreements (SLAs) operation templates, all operation templates for a specified type of operation, or a specified operation template, use the **show ip sla auto template** command in user EXEC or privileged EXEC mode.

show ip sla auto template [**type ip** [*operation* [*template-name*]]]

Syntax Description

type ip	Specifies that the operation type is Internet Protocol (IP).
operation	Type of IP operation. Use one of the following keywords: • **icmp-echo**—Internet Control Message Protocol (ICMP) echo operation • **icmp-jitter—**Internet Control Message Protocol (ICMP) jitter operation • **tcp-connect—**Transmission Control Protocol (TCP) connection operation • **udp-echo—**User Datagram Protocol (UDP) echo operation • **udp-jitter—**User Datagram Protocol (UDP) jitter operation
template-name	Unique identifier of an IP SLAs operation template. String of 1 to 64 alphanumeric characters.

Command Default

Default output includes configuration for all auto IP SLAs operation templates.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following is sample shows output for the **show ip sla auto template** command when you specify a template by name (basic_icmp_jtr):

```
Router# show ip sla auto template type ip icmp-jitter basic_icmp_jtr
IP SLAs Auto Template: basic_icmp_jtr
    Measure Type: icmp-jitter
    Description: default oper temp for icmp jitter
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
```

```
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

The following is sample output for the **show ip sla auto template** command when you use the **type ip** *operation* keyword and argument combination to specifiy a certain type of operation:

```
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: basic_udp_jitter
    Measure Type: udp-jitter (control enabled)
    Description: default oper temp for udp jitter
    IP options:
        Source IP: 0.0.0.0 Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
IP SLAs Auto Template: voip_g711alaw
    Measure Type: udp-jitter (control enabled)
    Description: oper template for voip udp
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Verify Data: false
        Timeout: 5000           Threshold: 5000
        Codec: g711alaw Number of packets: 1000
        Interval: 20    Payload size: 16        Advantage factor: 0
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

The following is sample output for the **show ip sla auto template** command for all configured IP SLAs operation templates. Because all of the templates are for IP operations, the **type ip** keyword is not configured.

```
Router# show ip sla auto template
IP SLAs Auto Template: basic_icmp_echo
    Measure Type: icmp-echo
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 28   Verify Data: false
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
```

```
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
IP SLAs Auto Template: basic_icmp_jtr
    Measure Type: icmp-jitter
    Description: default oper temp for icmp jitter
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
IP SLAs Auto Template: basic_udp_jitter
    Measure Type: udp-jitter (control enabled)
    Description: default oper temp for udp jitter
    IP options:
        Source IP: 0.0.0.0 Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 32   Verify Data: false
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
IP SLAs Auto Template: voip_g711alaw
    Measure Type: udp-jitter (control enabled)
    Description: oper template for voip udp
    IP options:
        Source IP: 0.0.0.0 Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Verify Data: false
        Timeout: 5000           Threshold: 5000
        Codec: g711alaw Number of packets: 1000
        Interval: 20    Payload size: 16        Advantage factor: 0
        Granularity: msec       Operation packet priority: normal
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
IP SLAs Auto Template: basic_tcp_conn
    Measure Type: tcp-connect (control enabled)
    Description:
    IP options:
```

```
    Source IP: 0.0.0.0 Source Port: 0
    VRF:    TOS: 0x0
Operation Parameters:
    Timeout: 5000           Threshold: 5000
Statistics Aggregation option:
    Hours of statistics kept: 2
History options:
    History filter: none
    Max number of history records kept: 15
    Lives of history kept: 0
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

Table 32 describes the significant fields shown in the display.

Table 36 **show ip sla auto template *Field Descriptions***

Field	Description
IP SLAs Auto Template	Name of auto IP SLAs operation template in current display.
Measure Type	Type of IP operation defined for auto IP SLAs operation template in current display, including status of protocol control.

Related Commands

Command	Description
ip sla auto template	Begins configuring an auto IP SLAs operation template and enters IP SLA template configuration mode.

show ip sla configuration

To display configuration values including all defaults for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla configuration** command in user EXEC or privileged EXEC mode.

show ip sla configuration [*operation*]

Syntax Description

operation	(Optional) Number of the IP SLAs operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor configuration** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr configuration** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor configuration** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor configuration** command.
12.2(33)SRE	This command was modified. The command output has been modified to include information on IP SLAs Ethernet operation port level support.

Examples

The following sections show sample output from the **show ip sla configuration** command for different IP SLAs operations in IPv4 and IPv6 networks.

Output for ICMP Echo Operations

IP SLAs Internet Control Message Protocol (ICMP) echo operations support both IPv4 and IPv6 addresses.

The following example shows output from the **show ip sla configuration** command when the specified operation is an ICMP echo operation in an IPv4 network:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: echo
Target address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
```

```
Request size (ARR data portion): 28
Verify data: No
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

The following example shows output from the **show ip sla configuration** command when the specified operation is an ICMP echo operation in an IPv6 network:

```
Router# show ip sla configuration 1

IP SLAs, Infrastructure Engine-II.

Entry number: 1
Owner:
Tag:
Type of operation to perform: echo
Target address/Source address: 2001:DB8:100::1/2001:0DB8:200::FFFE
Traffic-Class parameter: 0x80
Flow-Label parameter: 0x1B669
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
```

Output for HTTP Operations

The following example shows output from the **show ip sla configuration** command when the specified operation is a Hypertext Transfer Protocol (HTTP) operation:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: http
Target address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
HTTP Operation: get
HTTP Server Version: 1.0
```

```
URL: http://www.cisco.com
Proxy:
Raw String(s):
Cache Control: enable
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for ICMP Path Jitter Operations

The following example shows output from the **show ip sla configuration** command when the specified operation is an ICMP path jitter operation:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: pathJitter
Target address/Source address: 1.1.1.1/0.0.0.0
Packet Interval/Number of Packets: 20 ms/10
Target Only: Disabled
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Loose Source Routing: Disabled
LSR Path:
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
```

Output for ICMP Path Echo Operations

The following example shows output from the **show ip sla configuration** command when the specified operation is an ICMP path echo operation:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: pathEcho
Target address/Source address: 1.1.1.1/0.0.0.0
Packet Interval/Number of Packets: 20 ms/10
Operation timeout (milliseconds): 5000
```

```
Type Of Service parameters: 0x0
Loose Source Routing: Disabled
Vrf Name:
LSR Path:
Request size (ARR data portion): 28
Verify data: No
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic paths kept: 5
   Number of statistic hops kept: 16
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for DNS Operations

The following example shows output from the **show ip sla configuration** command when the specified operation is a Domain Name System (DNS) operation:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: dns
Target Address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for UDP Echo Operations

IP SLAs User Datagram Protocol (UDP) echo operations support both IPv4 and IPv6 addresses.

The following example shows output from the **show ip sla configuration** command when the specified operation is a UDP echo operation in an IPv4 network:

```
Router# show ip sla configuration 3

Entry number: 3
```

```
Owner:
Tag:
Type of operation: udpEcho
Target address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Data Pattern:
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Control Packets: enabled
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

The following example shows output from the **show ip sla configuration** command when the specified operation is a UDP echo operation in an IPv6 network:

```
Router# show ip sla configuration 1

IP SLAs, Infrastructure Engine-II.

Entry number: 1
Owner:
Tag:
Type of operation to perform: udp-echo
Target address/Source address: 2001:DB8:100::1/2001:0DB8:200::FFFE
Target port/Source port: 3/7
Traffic-Class parameter: 0x80
Flow-Label parameter: 0x1B669
Request size (ARR data portion): 16
Operation timeout (milliseconds): 5000
Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
```

Output for TCP Connect Operations

IP SLAs Transmission Control Protocol (TCP) connect operations support both IPv4 and IPv6 addresses.

The following example shows output from the **show ip sla configuration** command when the specified operation is a TCP connect operation in an IPv4 network:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: tcpConnect
Target Address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Control Packets: enabled
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

The following example shows output from the **show ip sla configuration** command when the specified operation is a TCP connect operation in an IPv6 network:

```
Router# show ip sla configuration 1

IP SLAs, Infrastructure Engine-II.

Entry number: 1
Owner:
Tag:
Type of operation to perform: tcp-connect
Target address/Source address: 2001:DB8:100::1/2001:0DB8:200::FFFE
Target port/Source port: 3/7
Traffic-Class parameter: 0x80
Flow-Label parameter: 0x1B669
Operation timeout (milliseconds): 60000
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
```

Output for DHCP Operations

The following example shows output from the **show ip sla configuration** command when the specified operation is a Dynamic Host Configuration Protocol (DHCP) operation:

```
Router# show ip sla configuration 3
```

```
Entry number: 3
Owner:
Tag:
Type of operation: dhcp
Target Address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Dhcp option:
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for FTP Operations

The following example shows output from the **show ip sla configuration** command when the specified operation is a File Transfer Protocol (FTP) operation:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: ftp
Source address: 0.0.0.0
FTP URL: ftp://ipsla:ipsla@172.19.192.109/test.txt
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for UDP Jitter Operations

IP SLAs User Datagram Protocol (UDP) jitter connect operations support both IPv4 and IPv6 addresses.

The following example shows output from the **show ip sla configuration** command when the specified operation is a UDP jitter operation in an IPv4 network:

```
Router# show ip sla configuration 3

Entry number: 3
Owner:
```

```
Tag:
Type of operation: jitter
Target Address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Packet Interval/Number of Packets: 20 ms/10
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Control Packets: enabled
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Enhanced History:
```

The following example shows output from the **show ip sla configuration** command when the specified operation is a UDP jitter operation in an IPv6 network:

```
Router# show ip sla configuration 1

IP SLAs, Infrastructure Engine-II.

Entry number: 1
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 2001:DB8:100::1/2001:0DB8:200::FFFE
Target port/Source port: 3/7
Traffic-Class parameter: 0x0
Flow-Label parameter: 0x0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 30/15
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
```

Related Commands

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

show ip sla enhanced-history collection-statistics

To display enhanced history statistics for all collected history buckets for the specified Cisco IOS IP Service Level Agreements (SLAs) operation, use the **show ip sla enhanced-history collection-statistics** command in user EXEC or privileged EXEC mode.

show ip sla enhanced-history collection-statistics [*operation-number*] [**interval** *seconds*]

Syntax Description

operation-number	(Optional) Number of the operation for which enhanced history statistics is displayed.
interval *seconds*	(Optional) Displays enhanced history distribution statistics for only the specified aggregation interval.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor enhanced-history collection-statistics** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr enhanced-history collection-statistics** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor enhanced-history collection-statistics** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor enhanced-history collection-statistics** command.

Usage Guidelines

This command displays data for each bucket of enhanced history data. Data is shown individually (one after the other).

The number of buckets and the collection interval is set using the **history enhanced** command.

You can also use the following commands to display additional statistics or history information, or to view the status of the operation:

- **show ip sla enhanced-history distribution-statistics**
- **show ip sla statistics**
- **show ip sla statistics aggregated**

Tip If the letter n appears in your output, or not all fields are displayed, you should increase the screen width for your command line interface display (for example, using the **width** line configuration command or the **terminal width** EXEC mode command).

Examples

The following example shows sample output for the **show ip sla enhanced-history collection-statistics** command. The output of this command will vary depending on the type of IP SLAs operation.

```
Router# show ip sla enhanced-history collection-statistics 1

Entry number: 1
Aggregation Interval: 900

Bucket Index: 1
Aggregation start time 00:15:00.003 UTC Thur May 1 2003
Target Address:
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
 .
 .
 .
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip sla enhanced-history collection-statistics Field Descriptions

Field	Description
Aggregation Interval	The number of seconds the operation runs for each enhanced history bucket. For example, a value of 900 indicates that statistics were gathered for 15 minutes before the next bucket was created.
Bucket Index	The number identifying the collection bucket. The number of buckets is set using the **history enhanced** IP SLA configuration command.

Related Commands

Command	Description
ip sla	Allows configuration of IP SLA operations by entering IP SLA configuration mode for the specified operation number.
show ip sla enhanced-history distribution-statistics	Displays enhanced history distribution statistics for IP SLAs operations in tabular format.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

show ip sla enhanced-history distribution-statistics

To display enhanced history distribution statistics for Cisco IOS IP Service Level Agreements (SLAs) operations in tabular format, use the **show ip sla enhanced-history distribution-statistics** command in user EXEC or privileged EXEC mode.

show ip sla enhanced-history distribution-statistics [*operation-number* [**interval** *seconds*]]

Syntax Description

operation-number	(Optional) Number of the operation for which enhanced history statistics is displayed.
interval *seconds*	(Optional) Displays enhanced history distribution statistics for only the specified aggregation interval for only the specified operation.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor enhanced-history distribution-statistics** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr enhanced-history distribution-statistics** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor enhanced-history distribution-statistics** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor enhanced-history distribution-statistics** command.

Usage Guidelines

The distribution statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completion times squared (used to calculate standard deviation)
- The maximum and minimum completion times
- The number of completed attempts

You can also use the following commands to display additional statistics or history information, or to view the status of the operation:

- **show ip sla enhanced-history collection-statistics**
- **show ip sla statistics**
- **show ip sla statistics aggregated**

Tip If the letter n appears in your output, or not all fields are displayed, you should increase the screen width for your command line interface display (for example, using the **width** line configuration command or the **terminal width** EXEC mode command).

Examples

The following is sample output from the **show ip sla enhanced-history distribution-statistics** command. The fields are defined at the beginning of the output for the command. RTT means round-trip time.

```
Router# show ip sla enhanced-history distribution-statistics 3

 Point by point Enhanced History

Entry    = Entry Number
Int      = Aggregation Interval (seconds)
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT    Pth Hop Comps OvrTh SumCmp   SumCmp2L  SumCmp2H   TMax     TMin
3     900 1    257850000 1   1   3     0     43       617        0          15       14
3     900 2    258750002 1   1   3     0     45       677        0          16       14
3     900 3    259650000 1   1   3     0     44       646        0          15       14
3     900 4    260550002 1   1   3     0     42       594        0          15       12
3     900 5    261450003 1   1   3     0     42       590        0          15       13
3     900 6    262350001 1   1   3     0     46       706        0          16       15
3     900 7    263250003 1   1   3     0     46       708        0          16       14
 .
 .
 .
```

The time elapsed between BucketIndex 1 (started at 257,850,000) and BucketIndex 2 (started at 258,750,002) in this example is 900,002 milliseconds, or 900 seconds.

Table 38 describes the significant fields shown in the display.

Table 38 show ip sla enhanced-history distribution-statistics Field Descriptions

Field	Description
Entry	The operation ID number you specified for the IP SLAs operation.
Int	Aggregation interval—The configured statistical distribution buckets interval, in seconds. For example, a value of 900 for Int means that statistics are gathered for 900 seconds per bucket.

Table 38 show ip sla enhanced-history distribution-statistics Field Descriptions (continued)

Field	Description
BucI	Bucket index number—A number uniquely identifying the statistical distribution (aggregation) bucket. The number of history buckets to be kept is configured using the **history buckets-kept** command. A bucket will gather statistics for the specified interval of time (aggregation interval), after which a new statistics bucket is created. If a number-of-buckets-kept value is configured, the interval for the last bucket is infinity (until the end of the operation). Buckets are not applicable to HTTP and UDP jitter monitoring operations. This field is equivalent to the rttMonStatsCaptureDistIndex object in the Cisco RTTMON MIB.
StartT	Aggregation start time—Start time for the aggregation interval (per Bucket Index). Shows the start time as the number of milliseconds since the router started; in other words, the time stamp is the number of milliseconds since the last system bootup.
Pth	Path index number—An identifier for a set of different paths to the target destination that have been discovered. For example, if the first operation iteration finds the path h1, h2, h3, h4, then this path is labeled as 1. If, on a later iteration, a new path is discovered, (such as h1, h2, h5, h6, h4) then this new path will be identified as 2, and so on. Data collection per path is available only for ICMP path echo operations ("pathEcho probes"). For all other operations, a value of 1 will always appear. Data collection per path is configured using the **paths-of-statistics-kept** *number* command when configuring the operation.
Hop	Hop Index Number—Statistics data per hop. A hop is data transmission between two points in a path (for example, from device h2 to device h3). Data collection per hop is available only for ICMP path echo operations ("pathEcho probes"). For all other operations, a value of "1" will always appear. Data collection per hop is configured using the **hops-of-statistics-kept** *number* command when configuring the operation. This field is equivalent to the rrttMonStatsCaptureHopIndex object in the Cisco RTTMON MIB.

Table 38 show ip sla enhanced-history distribution-statistics Field Descriptions (continued)

Field	Description
Comps	Completions—The number of round-trip time operations that have completed without an error and without timing out, per bucket index. This object has the special behavior as defined by the ROLLOVER NOTE in the DESCRIPTION of the Cisco Rttmon MIB object.
SumCmp	Sum of completed operation times (1)—The total of all round-trip time values for all successful operations in the row, in milliseconds.
SumCmp2L	Sum of the squares of completed operation times (2), Low-Order—The sum of the square roots of round-trip times for operations that were successfully measured, in milliseconds; displays the low-order 32 bits of the value only. • 32 low-order bits and 32 high-order bits are ordered in unsigned 64-bit integers (Int64) as follows: --- | High-order 32 bits | Low-order 32 bits | --- • The "SumCmp2" values are split into "high-order" and "low-order" numbers because of limitations of Simple Network Management Protocol (SNMP). The maximum value allowed for an SNMP object is 4,294,967,295 (the Gauge32 limit). If the sum of the square roots for your operation exceeds this value, then the "high-order" value will be utilized. (For example, the number 4,294,967,296 would have all low-order bits as 0, and the right-most high-order bit would be 1). • The low-order value (SumCmp2L) appears first in the output because in most cases, the value will be less than 4,294,967,295, which means that the value of SumCmp2H will appear as zero.
SumCmp2H	Sum of the squares of completed operation times (2), High-Order—The high-order 32 bits of the accumulated squares of completion times (in milliseconds) of operations that completed successfully.
TMax	Round-trip time, maximum—The highest recorded round-trip time, in milliseconds, per aggregation interval.
TMin	Round-trip time, minimum—The lowest recorded round-trip time, in milliseconds, per aggregation interval.

Related Commands

Command	Description
ip sla	Allows configuration of IP SLA operations by entering IP SLA configuration mode for the specified operation number.
show ip sla enhanced-history collection-statistics	Displays enhanced history statistics for all collected history buckets for the specified IP SLAs operation.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

show ip sla ethernet-monitor configuration

To display configuration settings for IP Service Level Agreements (SLAs) auto Ethernet operations, use the **show ip sla ethernet-monitor configuration** command in user EXEC or privileged EXEC mode.

show ip sla ethernet-monitor configuration [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the auto Ethernet operation for which the details will be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

If the identification number of an auto Ethernet operation is not specified, configuration values for all the configured auto Ethernet operations will be displayed.

Examples

The following is sample output from the **show ip sla ethernet-monitor configuration** command:

```
Router# show ip sla ethernet-monitor configuration 1

Entry Number : 1
Modification time   : *00:47:46.703 GMT Thu Jan 11 2007
Operation Type      : echo
Domain Name         : a
VLAN ID             : 11
Excluded MPIDs      :
Owner               :
Tag                 :
Timeout(ms)         : 5000
Threshold(ms)       : 5000
Frequency(sec)      : 60
Operations List     : Empty
Schedule Period(sec): 0
Request size        : 0
CoS                 : 0
Start Time          : Pending trigger
SNMP RowStatus      : notInService
Reaction Configs    :
 Reaction Index     : 1
 Reaction           : RTT
 Threshold Type     : Never
 Threshold Rising   : 300
```

```
Threshold Falling  : 200
Threshold CountX   : 5
Threshold CountY   : 5
Action Type        : None
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip sla ethernet-monitor configuration Field Descriptions

Field	Description
Entry Number	Identification number for the auto Ethernet operation.
Operation Type	Type of IP SLAs operation configured by the auto Ethernet operation.
Domain Name	Name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
VLAN ID	VLAN identification number
Excluded MPIDs	List of maintenance endpoint identification numbers to be excluded from the auto Ethernet operation.
Owner	Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Tag	User-specified identifier for an IP SLAs operation.
Timeout(ms)	Amount of time the IP SLAs operation waits for a response from its request packet.
Threshold(ms)	Upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Frequency(sec)	Time after which an individual IP SLAs operation is restarted.
Operations List	Identification numbers of the individual operations created by the auto Ethernet operation.
Schedule Period(sec)	Time period (in seconds) in which the start times of the individual Ethernet operations are distributed.
Request size	Padding size for the data frame of the individual operations created by the auto Ethernet operation.
CoS	Class of Service of the individual operations created by the auto Ethernet operation.
Start Time	Status of the start time for the auto Ethernet operation.
SNMP RowStatus	Indicates whether SNMP RowStatus is active or inactive.
Reaction Configs	Reaction configuration of the IP SLAs operation.
Reaction Index	Identification number used to identify different reaction configurations for an IP SLAs operation.
Reaction	Reaction condition being monitored.
Threshold Type	Specifies when an action should be performed as a result of a reaction event.

Table 39 show ip sla ethernet-monitor configuration Field Descriptions (continued)

Field	Description
Threshold Rising	The upper threshold value of the reaction condition being monitored. Corresponds to the *upper-threshold* argument of the **threshold-value** *upper-threshold lower-threshold* syntax in the **ip sla ethernet-monitor reaction-configuration** command.
Threshold Falling	The lower threshold value of the reaction condition being monitored. Corresponds to the *lower-threshold* argument of the **threshold-value** *upper-threshold lower-threshold* syntax in the **ip sla ethernet-monitor reaction-configuration** command.
Threshold CountX	Corresponds to the *x-value* argument of the **threshold-type xofy** *x-value y-value* syntax in the **ip sla ethernet-monitor reaction-configuration** command.
Threshold CountY	Corresponds to the *y-value* argument of the **threshold-type xofy** *x-value y-value* syntax in the **ip sla ethernet-monitor reaction-configuration** command.
Action Type	Type of action that should be performed as a result of a reaction event.

Related Commands

Command	Description
ip sla ethernet-monitor	Begins configuration for an IP SLAs auto Ethernet operation and enters Ethernet monitor configuration mode.
ip sla ethernet-monitor reaction-configuration	Configures the proactive threshold monitoring parameters for an IP SLAs auto Ethernet operation.
ip sla ethernet-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.

show ip sla event-publisher

To display the list of client applications that are registered to receive IP Service Level Agreements (SLAs) notifications, use the **show ip sla event-publisher** command in user EXEC or privileged EXEC mode.

show ip sla event-publisher

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

The following is sample output from the **show ip sla event-publisher** command:

```
Router# show ip sla event-publisher

client-id  process-id  event-type
------------------------------------
appl1      1111        react-alert
appl1      1221        react-alert
appl1      1331        react-alert

Router#
```

Table 40 describes the fields shown in the display.

Table 40 show ip sla event-publisher Field Descriptions

Field	Description
client-id	The identity of the client registered to receive IP SLAs notifications.
process-id	The process identity associated with the client.
event-type	The type of notification (event) that the client has registered to receive.

Related Commands

Command	Description
ip sla enable reaction-alerts	Enables IP SLA notifications to be sent to all registered applications.
show ip sla application	Displays global information about Cisco IOS IP SLAs.

show ip sla group schedule

To display the group schedule details for Cisco IOS IP Service Level Agreements (SLAs) operations, use the **show ip sla group schedule** command in user EXEC or privileged EXEC mode.

show ip sla group schedule [*group-operation-number*]

Syntax Description

group-operation-number	(Optional) Number of the IP SLAs group operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor group schedule** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr group schedule** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor group schedule** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor group schedule** command.

Examples

The following is sample output from the **show ip sla group schedule** command that shows information about group (multiple) scheduling. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE):

```
Router# show ip sla group schedule

Multi-Scheduling Configuration:
Group Entry Number: 1
Probes to be scheduled: 2,3,4,9-30,89
Schedule period :60
Group operation frequency: 30
Multi-scheduled: TRUE
```

The following is sample output from the **show ip sla group schedule** command that shows information about group (multiple) scheduling, with the frequency value the same as the schedule period value, the life value as 3600 seconds, and the ageout value as never:

```
Router# show ip sla group schedule
Group Entry Number: 1
Probes to be scheduled: 3,4,6-10
Total number of probes: 7
Schedule period: 20
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 3600
```

```
Entry Ageout (seconds): never
```

Table 41 describes the significant fields shown in the displays.

Table 41 show ip sla group schedule Field Descriptions

Field	Description
Group Entry Number	The operation group number specified for IP SLAs multiple operations scheduling.
Probes to be scheduled	The operations numbers specified in the operation group 1.
Scheduled period	The time (in seconds) for which the IP SLAs group is scheduled.
Group operation frequency	The frequency at which each operation is started.
Multi-scheduled	The value TRUE shows that group scheduling is active.

Related Commands

Command	Description
show ip sla configuration	Displays the configuration details for IP SLAs operations.

show ip sla history

To display history collected for all Cisco IOS IP Service Level Agreements (SLAs) operations or for a specified operation, use the **show ip sla history** command in user EXEC or privileged EXEC mode.

show ip sla history [*operation-number*] [**tabular** | **full**]

Syntax Description

operation-number	(Optional) Number of the operation for which history details is displayed.
tabular	(Optional) Displays information in a column format, reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information, using identifiers next to each displayed value.

Defaults

Tabular format history for all operations is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor history** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr history** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor history** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor history** command.

Usage Guidelines

Table 42 lists the Response Return values used in the output of the **show ip sla history** command. If the default (tabular) format is used, the Response Return description is displayed as a code in the Sense column. If the full format is used, the Response Return is displayed as indicated in the Description column.

Table 42 Response Return (Sense Column) Codes

Code	Description
1	Okay.
2	Disconnected.
3	Over threshold.
4	Timeout.

Table 42 Response Return (Sense Column) Codes (continued)

Code	Description
5	Busy.
6	Not connected.
7	Dropped.
8	Sequence error.
9	Verify error.
10	Application specific.

Examples

The following is sample output from the **show ip sla history** command in tabular format.

Note Prior to Cisco IOS Release 12.4(24)T, the value for Sample Start Time was displayed in centiseconds. In Cisco IOS Release 12.4(24)T and later releases, the value for Sample Start Time is displayed in milliseconds as shown in the following sample output.

```
Router# show ip sla history

        Point by point History
          Multiple Lines per Entry
Line 1
 Entry    = Entry Number
 LifeI    = Life Index
 BucketI  = Bucket Index
 SampleI  = Sample Index
 SampleT  = Sample Start Time (milliseconds)
 CompT    = Completion Time (milliseconds)
 Sense    = Response Return Code
Line 2 has the Target Address
Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense
2     1          1          1          174365480   16          1
  AB 45 A0 16
2     1          2          1          174365510   4           1
  AC 12 7  29
2     1          2          2          174365510   1           1
  AC 12 5  22
2     1          2          3          174365520   4           1
  AB 45 A7 22
2     1          2          4          174365520   4           1
  AB 45 A0 16
```

Related Commands

Command	Description
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla monitor application

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor application** command is replaced by the **show ip sla application** command. See the **show ip sla application** command for more information.

To display global information about Cisco IOS IP Service Level Agreements (SLAs), use the **show ip sla monitor application** command in user EXEC or privileged EXEC mode.

show ip sla monitor application [**tabular** | **full**]

Syntax Description

tabular	(Optional) Displays information in a column format, reducing the number of screens required to display the information.
full	(Optional) Displays all information, using identifiers next to each displayed value. This is the default.

Defaults

Full format

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla application** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr application** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla application** command.
12.2(33)SXI	This command was replaced by the **show ip sla application** command.

Usage Guidelines

Use the **show ip sla monitor application** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show ip sla monitor application** command in full format:

```
Router# show ip sla monitor application

        IP Service Level Agreement Monitor
Version: 2.2.0 Round Trip Time MIB
Time of last change in whole IP SLA Monitor: *17:21:30.819 UTC Tue Mar 19 2002
Estimated system max number of entries: 4699
```

```
Number of Entries configured:5
    Number of active Entries:5
   Number of pending Entries:0
  Number of inactive Entries:0
         Supported Operation Types
Type of Operation to Perform:  echo
Type of Operation to Perform:  pathEcho
Type of Operation to Perform:  udpEcho
Type of Operation to Perform:  tcpConnect
Type of Operation to Perform:  http
Type of Operation to Perform:  dns
Type of Operation to Perform:  jitter
Type of Operation to Perform:  dlsw
Type of Operation to Perform:  dhcp
Type of Operation to Perform:  ftp

        Supported Protocols
Protocol Type: ipIcmpEcho
Protocol Type: ipUdpEchoAppl
Protocol Type: snaRUEcho
Protocol Type: snaLU0EchoAppl
Protocol Type: snaLU2EchoAppl
Protocol Type: ipTcpConn
Protocol Type: httpAppl
Protocol Type: dnsAppl
Protocol Type: jitterAppl
Protocol Type: dlsw
Protocol Type: dhcp
Protocol Type: ftpAppl

Number of configurable probe is 490
```

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla monitor authentication

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor authentication** command is replaced by the **show ip sla authentication** command. See the **show ip sla authentication** command for more information.

To display Cisco IOS IP Service Level Agreements (SLAs) authentication information, use the **show ip sla monitor authentication** command in user EXEC or privileged EXEC mode.

show ip sla monitor authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla authentication** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr authentication** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla authentication** command.
12.2(33)SXI	This command was replaced by the **show ip sla authentication** command.

Usage Guidelines

Use the **show ip sla monitor authentication** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show ip sla monitor authentication** command:

```
Router# show ip sla monitor authentication

IP SLA Monitor control message uses MD5 authentication, key chain name is: ipsla
```

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values for IP SLAs operations.

show ip sla monitor collection-statistics

Note Effective with Cisco IOS Release 12.4(2)T, the **show ip sla monitor collection-statistics** command is replaced by the **show ip sla monitor statistics aggregated** command. See the **show ip sla monitor statistics aggregated** command for more information.

To display statistical errors for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla monitor collection-statistics** command in user EXEC or privileged EXEC mode.

show ip sla monitor collection-statistics [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was replaced by the **show ip sla monitor statistics aggregated** command.

Usage Guidelines

Use the **show ip sla monitor collection-statistics** command to display information such as the number of failed operations and the failure reason. You can also use the **show ip sla monitor distribution-statistics** and **show ip sla monitor totals-statistics** commands to display additional statistical information.

This command shows information collected over the past two hours, unless you specify a different amount of time using the **hours-of-statistics-kept** command.

For one-way delay jitter operations, the clocks on each device must be synchronized using Network Time Protocol (NTP) or global positioning systems. If the clocks are not synchronized, one-way measurements are discarded. (If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round-trip time, the one-way measurement values are assumed to be faulty, and are discarded.)

Note This command does not support the IP SLAs ICMP path jitter operation.

Examples

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

```
Router# show ip sla monitor collection-statistics 1

        Collected Statistics
Entry Number: 1
```

```
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Path Index: 1
Hop in Path Index: 1
Number of Failed Operations due to a Disconnect: 0
Number of Failed Operations due to a Timeout: 0
Number of Failed Operations due to a Busy: 0
Number of Failed Operations due to a No Connection: 0
Number of Failed Operations due to an Internal Error: 0
Number of Failed Operations due to a Sequence Error: 0
Number of Failed Operations due to a Verify Error: 0
Target Address: 172.16.1.176
```

Output for HTTP Operations

The following is output from the **show ip sla monitor collection-statistics** command when the specified operation is an HTTP operation:

```
Router# show ip sla monitor collection-statistics 2

        Collected Statistics

Entry Number:2
HTTP URL:http://172.20.150.200
Start Time:*00:01:16.000 UTC Mon Nov 1 2003

             Comps:1              RTTMin:343
             OvrTh:0              RTTMax:343
        DNSTimeOut:0              RTTSum:343
        TCPTimeOut:0             RTTSum2:117649
        TraTimeOut:0              DNSRTT:0
          DNSError:0           TCPConRTT:13
         HTTPError:0            TransRTT:330
           IntError:0           MesgSize:1771
             Busies:0
```

Output for UDP Jitter Operations

The following is sample output from the **show ip sla monitor collection-statistics** command, where operation 2 is a jitter operation that includes one-way statistics. Table 43 describes the significant fields shown in the display.

```
Router# show ip sla monitor collection-statistics

Collected Statistics

Entry Number: 2
Target Address: 5.0.0.1, Port Number:99
Start Time: 11:12:03.000 UTC Thu Jul 1 1999
RTT Values:
NumOfRTT: 600  RTTSum: 3789  RTTSum2: 138665
Packet Loss Values:
PacketLossSD: 0  PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
InternalError: 0  Busies: 0
Jitter Values:
MinOfPositivesSD: 1   MaxOfPositivesSD: 2
NumOfPositivesSD: 26  SumOfPositivesSD: 31   Sum2PositivesSD: 41
MinOfNegativesSD: 1   MaxOfNegativesSD: 4
NumOfNegativesSD: 56  SumOfNegativesSD: 73   Sum2NegativesSD: 133
MinOfPositivesDS: 1   MaxOfPositivesDS: 338
NumOfPositivesDS: 58  SumOfPositivesDS: 409  Sum2PositivesDS: 114347
MinOfNegativesDS: 1   MaxOfNegativesDS: 338
NumOfNegativesDS: 48  SumOfNegativesDS: 396  Sum2NegativesDS: 114332
One Way Values:
```

```
NumOfOW: 440
OWMinSD: 2  OWMaxSD: 6    OWSumSD: 1273  OWSum2SD: 4021
OWMinDS: 2  OWMaxDS: 341  OWSumDS: 1643  OWSum2DS: 120295
```

Output for UDP Jitter (codec) Operations

The following is sample output from the **show ip sla monitor collection-statistics** command, where operation 10 is a UDP jitter (codec) operation. Table 43 describes the significant fields shown in the display.

```
Router# show ip sla monitor collection-statistics 10

Entry Number: 10

Start Time Index: 12:57:45.931 UTC Wed Mar 12 2003
Number of successful operations: 60
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
Voice Scores:
 MinOfICPIF: 2   MaxOfICPIF:  20   MinOfMos: 3.20   MaxOfMos: 4.80
RTT Values:
 NumOfRTT: 600  RTTSum: 3789  RTTSum2: 138665
 Packet Loss Values:
 PacketLossSD: 0  PacketLossDS: 0
 PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
 InternalError: 0  Busies: 0
Jitter Values:
 NumOfJitterSamples: 540
 MinOfPositivesSD: 1   MaxOfPositivesSD: 2
 NumOfPositivesSD: 26  SumOfPositivesSD: 31   Sum2PositivesSD: 41
 MinOfNegativesSD: 1   MaxOfNegativesSD: 4
 NumOfNegativesSD: 56  SumOfNegativesSD: 73   Sum2NegativesSD: 133
 MinOfPositivesDS: 1   MaxOfPositivesDS: 338
 NumOfPositivesDS: 58  SumOfPositivesDS: 409  Sum2PositivesDS: 114347
 MinOfNegativesDS: 1   MaxOfNegativesDS: 338
 NumOfNegativesDS: 48  SumOfNegativesDS: 396  Sum2NegativesDS: 114332
 Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
 NumOfOW: 440
 OWMinSD: 2  OWMaxSD: 6    OWSumSD: 1273  OWSum2SD: 4021
 OWMinDS: 2  OWMaxDS: 341  OWSumDS: 1643  OWSum2DS: 120295
```

Table 43 show ip sla monitor collection-statistics Field Descriptions

Field	Description
Voice Scores	Indicates that Voice over IP statistics appear on the following lines. Voice score data is computed when the operation type is configured as **type jitter** (codec).
ICPIF	The Calculated Planning Impairment Factor (ICPIF) value for the operation. The ICPIF value is computed by IP SLAs using the formula *Icpif = Io + Iq + Idte + Idd + Ie – A*, where • The values for *Io*, *Iq*, and *Idte* are set to zero. • The value *Idd* is computed based on the measured one-way delay. • The value *Ie* is computed based on the measured packet loss. • The value of A is specified by the user. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically lower than 20 are generally considered "adequate." **Note** This value is intended only for relative comparisons, and may not match ICPIF values generated using alternate methods.
MinOfICPIF	The lowest (minimum) ICPIF value computed for the collected statistics.
MaxOfICPIF	The highest (maximum) ICPIF value computed for the collected statistics.
Mos	The estimated Mean Opinion Score (Conversational Quality, Estimated) for the latest iteration of the operation. The MOS-CQE is computed by IP SLAs as a function of the ICPIF. MOS values are expressed as a number from 1 (1.00) to 5 (5.00), with 5 being the highest level of quality, and 1 being the lowest level of quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.
MinOfMos	The lowest (minimum) MOS value computed for the collected statistics.
MaxOfMos	The highest (maximum) ICPIF value computed for the collected statistics.
RTT Values	Indicates that round-trip-time statistics appear on the following lines.
NumOfRTT	The number of successful round-trips.
RTTSum	The sum of all successful round-trip values (in milliseconds).

Table 43 show ip sla monitor collection-statistics Field Descriptions (continued)

Field	Description
RTTSum2	The sum of squares of those round-trip values (in milliseconds).
PacketLossSD	The number of packets lost from source to destination.
PacketLossDS	The number of packets lost from destination to source.
PacketOutOfSequence	The number of packets returned out of order.
PacketMIA	The number of packets lost where the direction (SD/DS) cannot be determined.
PacketLateArrival	The number of packets that arrived after the timeout.
InternalError	The number of times an operation could not be started due to other internal failures.
Busies	The number of times this operation could not be started because the previously scheduled run was not finished.
Jitter Values:	Indicates that jitter statistics appear on the following lines. Jitter is interpacket delay variance.
NumOfJitterSamples	The number of jitter samples collected. This is the number of samples that are used to calculate the following jitter statistics.
MinOfPositivesSD MaxOfPositivesSD	The minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	The number of jitter values from source to destination that are positive (that is, network latency increases for two consecutive test packets).
SumOfPositivesSD	The sum of those positive values (in milliseconds).
Sum2PositivesSD	The sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	The minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	The number of jitter values from source to destination that are negative (that is, network latency decreases for two consecutive test packets).
SumOfNegativesSD	The sum of those values.
Sum2NegativesSD	The sum of the squares of those values.
Interarrival jitterout	The source-to-destination (SD) jitter value calculation, as defined in RFC 1889.

Table 43 show ip sla monitor collection-statistics Field Descriptions (continued)

Field	Description
Interarrival jitterin	The destination-to-source (DS) jitter value calculation, as defined in RFC 1889.
One Way Values	Indicates that one-way measurement statistics appear on the following lines. One Way (OW) values are the amount of time required for the packet to travel from the source router to the target router (SD) or from the target router to the source router (DS).
NumOfOW	Number of successful one-way time measurements.
OWMinSD	Minimum time (in milliseconds) from the source to the destination.
OWMaxSD	Maximum time (in milliseconds) from the source to the destination.
OWSumSD	Sum of the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show ip sla monitor distributions-statistics	Displays statistics distribution information (captured response times) for all IP SLAs operations or the specified operation.
show ip sla monitor totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all IP SLAs operations or the specified operation.
show ntp status	Displays the status of the NTP configuration on your system.

show ip sla monitor configuration

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor configuration** command is replaced by the **show ip sla configuration** command. See the **show ip sla configuration** command for more information.

To display configuration values including all defaults for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla monitor configuration** command in user EXEC or privileged EXEC mode.

show ip sla monitor configuration [*operation*]

Syntax Description

operation	(Optional) Number of the IP SLAs operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	The displayed information was reorganized.
12.4(4)T	This command was replaced by the **show ip sla configuration** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr configuration** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla configuration** command.
12.2(33)SXI	This command was replaced by the **show ip sla configuration** command.

Examples

The following sections show sample output from the **show ip sla monitor configuration** command for different IP SLAs operations.

Output for ICMP Echo Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is an Internet Control Message Protocol (ICMP) echo operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: echo
Target address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
```

```
Request size (ARR data portion): 28
Verify data: No
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

Output for HTTP Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a Hypertext Transfer Protocol (HTTP) operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: http
Target address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
HTTP Operation: get
HTTP Server Version: 1.0
URL: http://www.cisco.com
Proxy:
Raw String(s):
Cache Control: enable
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for ICMP Path Jitter Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is an ICMP path jitter operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
```

```
Tag:
Type of operation: pathJitter
Target address/Source address: 1.1.1.1/0.0.0.0
Packet Interval/Number of Packets: 20 ms/10
Target Only: Disabled
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Loose Source Routing: Disabled
LSR Path:
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
```

Output for ICMP Path Echo Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is an ICMP path echo operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: pathEcho
Target address/Source address: 1.1.1.1/0.0.0.0
Packet Interval/Number of Packets: 20 ms/10
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Loose Source Routing: Disabled
Vrf Name:
LSR Path:
Request size (ARR data portion): 28
Verify data: No
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic paths kept: 5
   Number of statistic hops kept: 16
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for DNS Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a Domain Name System (DNS) operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: dns
Target Address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for UDP Echo Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a UDP echo operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: udpEcho
Target address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Data Pattern:
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Control Packets: enabled
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

Output for TCP Connect Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a Transmission Control Protocol (TCP) connect operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: tcpConnect
Target Address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Control Packets: enabled
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

Output for DHCP Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a Dynamic Host Configuration Protocol (DHCP) operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: dhcp
Target Address/Source address: 1.1.1.1/0.0.0.0
Operation timeout (milliseconds): 5000
Dhcp option:
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for FTP Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a File Transfer Protocol (FTP) operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: ftp
Source address: 0.0.0.0
FTP URL: ftp://ipsla:ipsla@172.19.192.109/test.txt
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
```

Output for UDP Jitter Operations

The following example shows output from the **show ip sla monitor configuration** command when the specified operation is a User Datagram Protocol (UDP) jitter operation:

```
Router# show ip sla monitor configuration 3

Entry number: 3
Owner:
Tag:
Type of operation: jitter
Target Address/Source address: 1.1.1.1/0.0.0.0
Target Port/Source Port: 1111/0
Packet Interval/Number of Packets: 20 ms/10
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
Request size (ARR data portion): 28
Verify data: No
Control Packets: enabled
Schedule:
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled: False
   Operation frequency (seconds): 60
   Life/Entry Ageout (seconds): Forever/never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (ms): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Enhanced History:
```

Related Commands

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

show ip sla monitor distributions-statistics

Note Effective with Cisco IOS Release 12.4(2)T, the **show ip sla monitor distributions-statistics** command is replaced by the **show ip sla monitor statistics aggregated details** command. See the **show ip sla monitor statistics aggregated** command for more information.

To display distribution statistics (captured response times) for all Cisco IOS IP Service Level Agreements (SLAs) operations or the specified operation, use the **show ip sla monitor distributions-statistics** command in user EXEC or privileged EXEC mode.

show ip sla monitor distributions-statistics [*operation*] [**tabular** | **full**]

Syntax Description

operation	(Optional) Number of the IP SLAs operation to display.
tabular	(Optional) Displays information in a column format, reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information, using identifiers next to each displayed value.

Defaults

Statistics are displayed for the past two hours.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was replaced by the **show ip sla monitor statistics aggregated details** command.

Usage Guidelines

The distribution statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completion times squared (used to calculate standard deviation)
- The maximum and minimum completion time
- The number of completed attempts

Note This command does not support the IP SLAs ICMP path jitter operation.

This command shows information collected over the past two hours, unless you specify a different amount of time using the **hours-of-statistics-kept** command.

You can also use the **show ip sla monitor collection-statistics** and **show ip sla monitor totals-statistics** commands to display additional statistical information.

Examples

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

```
Router# show ip sla monitor distributions-statistics

        Captured Statistics
        Multiple Lines per Entry
Line 1
Entry    = Entry Number
StartT   = Start Time of Entry (hundredths of seconds)
Pth      = Path Index
Hop      = Hop in Path Index
Dst      = Time Distribution Index
Comps    = Operations Completed
OvrTh    = Operations Completed Over Thresholds
SumCmp   = Sum of Completion Times (milliseconds)
Line 2
SumCmp2L = Sum of Completion Times Squared Low 32 Bits (milliseconds)
SumCmp2H = Sum of Completion Times Squared High 32 Bits (milliseconds)
TMax     = Completion Time Maximum (milliseconds)
TMin     = Completion Time Minimum (milliseconds)
Entry StartT   Pth Hop Dst Comps  OvrTh   SumCmp    SumCmp2L   SumCmp2H  TMax     TMin
1     17417068 1   1   1   2      0       128       8192       0         64       64
```

The fields shown in the display are self-explanatory.

Related Commands

Command	Description
show ip sla monitor collection-statistics	Displays statistical errors for all IP SLAs operations or the specified operation.
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show ip sla monitor totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all IP SLAs operations or the specified operation.

show ip sla monitor enhanced-history collection-statistics

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor enhanced-history collection-statistics** command is replaced by the **show ip sla enhanced-history collection-statistics** command. See the **show ip sla enhanced-history collection-statistics** command for more information.

To display enhanced history statistics for all collected history buckets for the specified Cisco IOS IP Service Level Agreements (SLAs) operation, use the **show ip sla monitor enhanced-history collection-statistics** command in user EXEC or privileged EXEC mode.

show ip sla monitor enhanced-history collection-statistics [*operation-number*] [**interval** *seconds*]

Syntax Description

operation-number	(Optional) Number of the operation for which enhanced history statistics is displayed.
interval *seconds*	(Optional) Displays enhanced history distribution statistics for only the specified aggregation interval.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla enhanced-history collection-statistics** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr enhanced-history collection-statistics** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla enhanced-history collection-statistics** command.
12.2(33)SXI	This command was replaced by the **show ip sla enhanced-history collection-statistics** command.

Usage Guidelines

This command displays data for each bucket of enhanced history data. Data is shown individually (one after the other).

The number of buckets and the collection interval is set using the **enhanced-history** command.

You can also use the following commands to display additional statistics or history information, or to view the status of the operation:

- **show ip sla monitor enhanced-history distribution-statistics**
- **show ip sla monitor statistics**
- **show ip sla monitor statistics aggregated**

Tip If the letter n appears in your output, or not all fields are displayed, you should increase the screen width for your command line interface display (for example, using the **width** line configuration command or the **terminal width** EXEC mode command).

Examples

The following example shows sample output for the **show ip sla monitor enhanced-history collection-statistics** command. The output of this command will vary depending on the type of IP SLAs operation.

```
Router# show ip sla monitor enhanced-history collection-statistics 1

Entry number: 1
Aggregation Interval: 900

Bucket Index: 1
Aggregation start time 00:15:00.003 UTC Thur May 1 2003
Target Address:
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
 .
 .
 .
```

Table 44 describes the significant fields shown in the display.

Table 44 show ip sla monitor enhanced-history collection-statistics Field Descriptions

Field	Description
Aggregation Interval	The number of seconds the operation runs for each enhanced history bucket. For example, a value of 900 indicates that statistics were gathered for 15 minutes before the next bucket was created.
Bucket Index	The number identifying the collection bucket. The number of buckets is set using the **enhanced-history** IP SLA monitor configuration command.

Related Commands

Command	Description
ip sla monitor	Allows configuration of IP SLA operations by entering IP SLA monitor configuration mode for the specified operation number.
show ip sla monitor enhanced-history distribution-statistics	Displays enhanced history distribution statistics for IP SLAs operations in tabular format.
show ip sla monitor statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla monitor statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

show ip sla monitor enhanced-history distribution-statistics

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor enhanced-history distribution-statistics** command is replaced by the **show ip sla enhanced-history distribution-statistics** command. See the **show ip sla enhanced-history distribution-statistics** command for more information.

To display enhanced history distribution statistics for Cisco IOS IP Service Level Agreements (SLAs) operations in tabular format, use the **show ip sla monitor enhanced-history distribution-statistics** command in user EXEC or privileged EXEC mode.

show ip sla monitor enhanced-history distribution-statistics [*operation-number* [**interval** *seconds*]]

Syntax Description

operation-number	(Optional) Number of the operation for which enhanced history statistics is displayed.
interval *seconds*	(Optional) Displays enhanced history distribution statistics for only the specified aggregation interval for only the specified operation.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla enhanced-history distribution-statistics** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr enhanced-history distribution-statistics** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla enhanced-history distribution-statistics** command.
12.2(33)SXI	This command was replaced by the **show ip sla enhanced-history distribution-statistics** command.

Usage Guidelines

The distribution statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completion times squared (used to calculate standard deviation)
- The maximum and minimum completion times
- The number of completed attempts

You can also use the following commands to display additional statistics or history information, or to view the status of the operation:

- **show ip sla monitor enhanced-history collection-statistics**
- **show ip sla monitor statistics**
- **show ip sla monitor statistics aggregated**

Tip If the letter n appears in your output, or not all fields are displayed, you should increase the screen width for your command line interface display (for example, using the **width** line configuration command or the **terminal width** EXEC mode command).

Examples

The following is sample output from the **show ip sla monitor enhanced-history distribution-statistics** command. The fields are defined at the beginning of the output for the command. RTT means round-trip time.

```
Router# show ip sla monitor enhanced-history distribution-statistics 3

 Point by point Enhanced History

Entry    = Entry Number
Int      = Aggregation Interval (seconds)
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT    Pth Hop Comps OvrTh SumCmp   SumCmp2L  SumCmp2H   TMax     TMin
3     900 1    257850000 1   1   3     0     43       617        0          15       14
3     900 2    258750002 1   1   3     0     45       677        0          16       14
3     900 3    259650000 1   1   3     0     44       646        0          15       14
3     900 4    260550002 1   1   3     0     42       594        0          15       12
3     900 5    261450003 1   1   3     0     42       590        0          15       13
3     900 6    262350001 1   1   3     0     46       706        0          16       15
3     900 7    263250003 1   1   3     0     46       708        0          16       14
 .
 .
 .
```

The time elapsed between BucketIndex 1 (started at 257,850,000) and BucketIndex 2 (started at 258,750,002) in this example is 900,002 milliseconds, or 900 seconds.

Table 45 describes the significant fields shown in the display.

Table 45 show ip sla monitor enhanced-history distribution-statistics Field Descriptions

Field	Description
Entry	The operation ID number you specified for the IP SLAs operation.
Int	Aggregation interval—The configured statistical distribution buckets interval, in seconds. For example, a value of 900 for Int means that statistics are gathered for 900 seconds per bucket.
BucI	Bucket index number—A number uniquely identifying the statistical distribution (aggregation) bucket. The number of history buckets to be kept is configured using the **buckets-of-history-kept** command. A bucket will gather statistics for the specified interval of time (aggregation interval), after which a new statistics bucket is created. If a number-of-buckets-kept value is configured, the interval for the last bucket is infinity (until the end of the operation). Buckets are not applicable to HTTP and UDP jitter monitoring operations. This field is equivalent to the rttMonStatsCaptureDistIndex object in the Cisco RTTMON MIB.
StartT	Aggregation start time—Start time for the aggregation interval (per Bucket Index). Shows the start time as the number of milliseconds since the router started; in other words, the time stamp is the number of milliseconds since the last system bootup.
Pth	Path index number—An identifier for a set of different paths to the target destination that have been discovered. For example, if the first operation iteration finds the path h1, h2, h3, h4, then this path is labeled as 1. If, on a later iteration, a new path is discovered, (such as h1, h2, h5, h6, h4) then this new path will be identified as 2, and so on. Data collection per path is available only for ICMP path echo operations (“pathEcho probes”). For all other operations, a value of 1 will always appear. Data collection per path is configured using the **paths-of-statistics-kept** *number* command when configuring the operation.

Table 45 show ip sla monitor enhanced-history distribution-statistics Field Descriptions

Field	Description
Hop	Hop Index Number—Statistics data per hop. A hop is data transmission between two points in a path (for example, from device h2 to device h3). Data collection per hop is available only for ICMP path echo operations ("pathEcho probes"). For all other operations, a value of "1" will always appear. Data collection per hop is configured using the **hops-of-statistics-kept** *number* command when configuring the operation. This field is equivalent to the rrttMonStatsCaptureHopIndex object in the Cisco RTTMON MIB.
Comps	Completions—The number of round-trip time operations that have completed without an error and without timing out, per bucket index. This object has the special behavior as defined by the ROLLOVER NOTE in the DESCRIPTION of the Cisco Rttmon MIB object.
SumCmp	Sum of completed operation times (1)—The total of all round-trip time values for all successful operations in the row, in milliseconds.
SumCmp2L	Sum of the squares of completed operation times (2), Low-Order—The sum of the square roots of round-trip times for operations that were successfully measured, in milliseconds; displays the low-order 32 bits of the value only. • 32 low-order bits and 32 high-order bits are ordered in unsigned 64-bit integers (Int64) as follows: --- | High-order 32 bits | Low-order 32 bits | --- • The "SumCmp2" values are split into "high-order" and "low-order" numbers because of limitations of Simple Network Management Protocol (SNMP). The maximum value allowed for an SNMP object is 4,294,967,295 (the Gauge32 limit). If the sum of the square roots for your operation exceeds this value, then the "high-order" value will be utilized. (For example, the number 4,294,967,296 would have all low-order bits as 0, and the right-most high-order bit would be 1). • The low-order value (SumCmp2L) appears first in the output because in most cases, the value will be less than 4,294,967,295, which means that the value of SumCmp2H will appear as zero.

Table 45 show ip sla monitor enhanced-history distribution-statistics Field Descriptions

Field	Description
SumCmp2H	Sum of the squares of completed operation times (2), High-Order—The high-order 32 bits of the accumulated squares of completion times (in milliseconds) of operations that completed successfully.
TMax	Round-trip time, maximum—The highest recorded round-trip time, in milliseconds, per aggregation interval.
TMin	Round-trip time, minimum—The lowest recorded round-trip time, in milliseconds, per aggregation interval.

Related Commands

Command	Description
ip sla monitor	Allows configuration of IP SLA operations by entering IP SLA monitor configuration mode for the specified operation number.
show ip sla monitor enhanced-history collection-statistics	Displays enhanced history statistics for all collected history buckets for the specified IP SLAs operation.
show ip sla monitor statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla monitor statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

show ip sla monitor group schedule

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor group schedule** command is replaced by the **show ip sla group schedule** command. See the **show ip sla group schedule** command for more information.

To display the group schedule details for Cisco IOS IP Service Level Agreements (SLAs) operations, use the **show ip sla monitor group schedule** command in user EXEC or privileged EXEC mode.

show ip sla monitor group schedule [*group-operation-number*]

Syntax Description

group-operation-number	(Optional) Number of the IP SLAs group operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla group schedule** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr group schedule** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla group schedule** command.
12.2(33)SXI	This command was replaced by the **show ip sla group schedule** command.

Examples

The following is sample output from the **show ip sla monitor group schedule** command that shows information about group (multiple) scheduling. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE):

```
Router# show ip sla monitor group schedule

Multi-Scheduling Configuration:
Group Entry Number: 1
Probes to be scheduled: 2,3,4,9-30,89
Schedule period :60
Group operation frequency: 30
Multi-scheduled: TRUE
```

The following is sample output from the **show ip sla monitor group schedule** command that shows information about group (multiple) scheduling, with the frequency value the same as the schedule period value, the life value as 3600 seconds, and the ageout value as never:

```
Router# show ip sla monitor group schedule
Group Entry Number: 1
Probes to be scheduled: 3,4,6-10
Total number of probes: 7
```

```
Schedule period: 20
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 3600
Entry Ageout (seconds): never
```

Table 46 describes the significant fields shown in the displays.

Table 46 show ip sla monitor group schedule Field Descriptions

Field	Description
Group Entry Number	The operation group number specified for IP SLAs multiple operations scheduling.
Probes to be scheduled	The operations numbers specified in the operation group 1.
Scheduled period	The time (in seconds) for which the IP SLAs group is scheduled.
Group operation frequency	The frequency at which each operation is started.
Multi-scheduled	The value TRUE shows that group scheduling is active.

Related Commands

Command	Description
show ip sla monitor configuration	Displays the configuration details for IP SLAs operations.

show ip sla monitor history

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor history** command is replaced by the **show ip sla history** command. See the **show ip sla history** command for more information.

To display history collected for all Cisco IOS IP Service Level Agreements (SLAs) operations or for a specified operation, use the **show ip sla monitor history** command in user EXEC or privileged EXEC mode.

show ip sla monitor history [*operation-number*] [**tabular** | **full**]

Syntax Description

operation-number	(Optional) Number of the operation for which history details is displayed.
tabular	(Optional) Displays information in a column format, reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information, using identifiers next to each displayed value.

Defaults

Tabular format history for all operations is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla history** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr history** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla history** command.
12.2(33)SXI	This command was replaced by the **show ip sla history** command.

Usage Guidelines

Table 47 lists the Response Return values used in the output of the **show ip sla monitor history** command. If the default (**tabular**) format is used, the Response Return description is displayed as a code in the Sense column. If the full format is used, the Response Return is displayed as indicated in the Description column.

Table 47 Response Return (Sense Column) Codes

Code	Description
1	Okay.
2	Disconnected.
3	Over threshold.
4	Timeout.
5	Busy.
6	Not connected.
7	Dropped.
8	Sequence error.
9	Verify error.
10	Application specific.

Examples

The following is sample output from the **show ip sla monitor history** command in tabular format:

```
Router# show ip sla monitor history

        Point by point History
          Multiple Lines per Entry
Line 1
 Entry    = Entry Number
 LifeI    = Life Index
 BucketI  = Bucket Index
 SampleI  = Sample Index
 SampleT  = Sample Start Time
 CompT    = Completion Time (milliseconds)
 Sense    = Response Return Code
Line 2 has the Target Address
Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense
2     1          1          1          17436548   16          1
  AB 45 A0 16
2     1          2          1          17436551   4           1
  AC 12 7  29
2     1          2          2          17436551   1           1
  AC 12 5  22
2     1          2          3          17436552   4           1
  AB 45 A7 22
2     1          2          4          17436552   4           1
  AB 45 A0 16
```

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

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

Note Effective with Cisco IOS Release 12.2(33)SB, the **show ip sla monitor mpls-lsp-monitor collection-statistics** command is replaced by the **show ip sla mpls-lsp-monitor collection-statistics** command. See the **show ip sla mpls-lsp-monitor collection-statistics** command for more information.

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SB	This command was replaced by the **show ip sla mpls-lsp-monitor collection-statistics** command.

Usage Guidelines

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

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

Examples

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

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

Entry number: 100001
Start Time Index: *19:32:37.995 EST Mon Feb 28 2005
Path Discovery Start Time: *20:23:43.919 EST Mon Feb 28 2005
Target destination IP address: 10.131.161.251
Path Discovery Status: OK
Path Discovery Completion Time: 1772
```

```
Path Discovery Minimum Paths: 12
Path Discovery Maximum Paths: 12
LSP Group Index: 100001
LSP Group Status: up
Total Pass: 1225
Total Timeout: 0 Total Fail: 0
Latest probe status: 'up,up,up,up,up,up,up,up,up,up,up,up'
Latest Path Identifier:
'127.0.0.13-Se3/0-38,127.0.0.6-Se3/0-38,127.0.0.1-Se3/0-38,127.0.0.2-Se3/0-38,127.0.0.4-Se
3/0-38,127.0.0.5-Se3/0-38,127.0.0.13-Se4/0-38,127.0.0.6-Se4/0-38,127.0.0.1-Se4/0-38,127.0.
0.2-Se4/0-38,127.0.0.4-Se4/0-38,127.0.0.5-Se4/0-38'
Minimum RTT: 24 Maximum RTT: 100 Average RTT: 42
```

Table 48 describes the significant fields shown in the display.

Table 48 show ip sla monitor mpls-lsp-monitor collection-statistics Field Descriptions

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

Table 48 show ip sla monitor mpls-lsp-monitor collection-statistics Field Descriptions

Field	Description
Maximum RTT	Maximum round-trip time (in milliseconds) measured by the IP SLAs operations associated with the specified LSP discovery group.
Average RTT	Average round-trip time (in milliseconds) for all the IP SLAs operations associated with the specified LSP discovery group.

Related Commands

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

show ip sla monitor mpls-lsp-monitor configuration

Note Effective with Cisco IOS Release 12.2(33)SB, the **show ip sla monitor mpls-lsp-monitor configuration** command is replaced by the **show ip sla mpls-lsp-monitor configuration** command. See the **show ip sla mpls-lsp-monitor configuration** command for more information.

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

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

Syntax Description

operation-number	(Optional) Number of the LSP Health Monitor operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced. This command replaces the **show rtr mpls-lsp-monitor configuration** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla mpls-lsp-monitor configuration** command.

Usage Guidelines

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

Examples

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

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

Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 1000
Threshold(ms)       : 5000
Frequency(sec)      : Equals schedule period
LSP Selector        : 127.0.0.1
ScanInterval(min)   : 1
Delete Scan Factor  : 1
```

```
Operations List     : 100001-100003
Schedule Period(sec): 60
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Secondary Frequency : Enabled on Timeout
         Value(sec) : 10
Reaction Configs    :
    Reaction        : connectionLoss
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
    Reaction        : timeout
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
```

The following is sample output from the **show ip sla monitor mpls-lsp-monitor configuration** command when the LSP discovery option is configured:

```
Router# show ip sla monitor mpls-lsp-monitor configuration 100

Entry Number : 100
Modification time   : *21:50:16.411 GMT Tue Jun 20 2006
Operation Type      : echo
Vrf Name            : saa-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 5000
Threshold(ms)       : 50
Frequency(sec)      : Equals schedule period
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100002
Schedule Period(sec): 30
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Path Discover       : Enable
    Maximum sessions          : 1
    Session Timeout(seconds)  : 120
    Base LSP Selector         : 127.0.0.1
    Echo Timeout(seconds)     : 5
    Send Interval(msec)       : 0
    Label Shimming Mode       : force-explicit-null
    Number of Stats Hours     : 2
    Scan Period(minutes)      : 3
Secondary Frequency : Enabled on Connection Loss and Timeout
         Value(sec) : 5
Reaction Configs    :
    Reaction        : Lpd Group
    Retry Number    : 3
    Action Type     : Trap Only
```

Table 49 describes the significant fields shown in the displays.

Table 49 show ip sla monitor mpls-lsp-monitor configuration Field Descriptions

Field	Description
Entry Number	Identification number for the LSP Health Monitor operation.
Operation Type	Type of IP SLAs operation configured by the LSP Health Monitor operation.
Vrf Name	If a specific name is displayed in this field, then the LSP Health Monitor is configured to discover only those Border Gateway Protocol (BGP) next hop neighbors in use by the VPN routing or forwarding instance (VRF) specified. If saa-vrf-all is displayed in this field, then the LSP Health Monitor is configured to discover all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router.
Tag	User-specified identifier for the LSP Health Monitor operation.
EXP Value	Experimental field value in the header for an echo request packet of the IP SLAs operation.
Timeout(ms)	Amount of time the IP SLAs operation waits for a response from its request packet.
Threshold(ms)	Threshold value of the IP SLAs operation for which a reaction event is generated if violated.
Frequency(sec)	Time after which the IP SLAs operation is restarted.
LSP Selector	Local host IP address used to select the LSP for the IP SLAs operation.
ScanInterval(min)	Time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.
Delete Scan Factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
Operations List	Identification numbers IP SLAs operations created by the LSP Health Monitor operation.
Schedule Period(sec)	Amount of time for which the LSP Health Monitor operation is scheduled.
Request size	Protocol data size for the request packet of the IP SLAs operation.
Start Time	Status of the start time for the LSP Health Monitor operation.
SNMP RowStatus	Indicates whether SNMP RowStatus is active or inactive.
TTL value	The maximum hop count for an echo request packet of the IP SLAs operation.
Reply Mode	Reply mode for an echo request packet of the IP SLAs operation.
Reply Dscp Bits	Differentiated services codepoint (DSCP) value of an echo reply packet of the IP SLAs operation.

Table 49 show ip sla monitor mpls-lsp-monitor configuration Field Descriptions (continued)

Field	Description
Path Discover	Indicates whether the LSP discovery option is enabled.
Maximum sessions	Maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation.
Session Timeout (seconds)	The amount of time the LSP discovery process waits for a response to its LSP discovery request for a particular BGP next hop neighbor.
Base LSP Selector	The base IP address used to select the LSPs of the LSP discovery groups.
Echo Timeout (seconds)	The amount of time the LSP discovery process waits for a response to its echo request packets.
Send Interval (msec)	The time interval (in milliseconds) between MPLS echo requests that are sent as part of the LSP discovery process.
Label Shimming Mode	Indicates whether the MPLS explicit null label option is enabled for the echo request packets.
Number of Stats Hours	The number of hours for which LSP discovery group statistics are maintained.
Scan Period (minutes)	The amount of time after which the LSP discovery process can restart.
Secondary Frequency	Reaction condition that will enable the secondary frequency option.
Value(sec)	Secondary frequency value.
Reaction Configs	The configured proactive threshold monitoring settings for the IP SLAs operation.
Reaction	Reaction condition being monitored.
Retry Number	Indicates the number of times the equal-cost multipaths belonging to an LSP discovery group are retested when a reaction condition is detected.
Threshold Type	Specifies when an action should be performed as a result of a reaction event.
Threshold Count	The number of times a reaction condition can occur before an action should be performed.
Action Type	Type of action that should be performed as a result of a reaction event.

Related Commands

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

Command	Description
auto ip sla mpls-lsp-monitor reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs LSP Health Monitor operation.
auto ip sla mpls-lsp-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.

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

Note Effective with Cisco IOS Release 12.2(33)SB, the **show ip sla monitor mpls-lsp-monitor lpd operational-state** command is replaced by the **show ip sla mpls-lsp-monitor lpd operational-state** command. See the **show ip sla mpls-lsp-monitor lpd operational-state** command for more information.

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SB	This command was replaced by the **show ip sla mpls-lsp-monitor lpd operational-state** command.

Usage Guidelines

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

Examples

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

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

Entry number: 100001
MPLSLM Entry Number: 1
Target FEC Type: LDP IPv4 prefix
Target Address: 192.168.1.11
Number of Statistic Hours Kept: 2
Last time LPD Stats were reset: *21:21:18.239 GMT Tue Jun 20 2006
Traps Type: 3
Latest Path Discovery Mode: rediscovery complete
Latest Path Discovery Start Time: *21:59:04.475 GMT Tue Jun 20 2006
Latest Path Discovery Return Code: OK
Latest Path Discovery Completion Time(ms): 3092
Number of Paths Discovered: 3
Path Information :
```

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

Table 50 describes the significant fields shown in the display.

Table 50 show ip sla monitor mpls-lsp-monitor lpd operational-state Field Descriptions

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

Related Commands

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

show ip sla monitor mpls-lsp-monitor neighbors

Note Effective with Cisco IOS Release 12.2(33)SB, the **show ip sla monitor mpls-lsp-monitor neighbors** command is replaced by the **show ip sla mpls-lsp-monitor neighbors** command. See the **show ip sla mpls-lsp-monitor neighbors** command for more information.

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

show ip sla monitor mpls-lsp-monitor neighbors

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced. This command replaces the **show rtr mpls-lsp-monitor neighbors** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla mpls-lsp-monitor neighbors** command.

Examples

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

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

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

Table 51 describes the significant fields shown in the display.

Table 51 show ip sla monitor mpls-lsp-monitor neighbors Field Descriptions

Field	Description
BGP Next hop	Identifier for the BGP next hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
ProbeID	The identification number of the IP SLAs operation. The names of the VPN routing or forwarding instances (VRFs) that contain routing entries for the specified BGP next hop neighbor are listed in parentheses.
OK	LSP ping or LSP traceroute connectivity status between the source Provider Edge (PE) router and specified BGP next hop neighbor. Connectivity status can be the following: • OK—Successful reply. • ConnectionLoss—Reply is from a device that is not egress for the Forward Equivalence Class (FEC). • Timeout—Echo request timeout. • Unknown—State of LSP is not known.

Related Commands

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

show ip sla monitor mpls-lsp-monitor scan-queue

Note Effective with Cisco IOS Release 12.2(33)SB, the **show ip sla monitor mpls-lsp-monitor scan-queue** command is replaced by the **show ip sla mpls-lsp-monitor scan-queue** command. See the **show ip sla mpls-lsp-monitor scan-queue** command for more information.

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

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

Syntax Description

operation-number	Number of the LSP Health Monitor operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced. This command replaces the **show rtr mpls-lsp-monitor scan-queue** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla mpls-lsp-monitor scan-queue** command.

Examples

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

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

Next scan Time after: 23 Secs
Next Delete scan Time after: 83 Secs

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

Table 52 describes the significant fields shown in the display.

Table 52 show ip sla monitor mpls-lsp-monitor scan-queue Field Descriptions

Field	Description
Next scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about adding BGP next hop neighbors to a particular VPN. At the start of each scan time, IP SLAs operations are created for all newly discovered neighbors.
Next Delete scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about deleting BGP next hop neighbors from a particular VPN. At the start of each delete scan time, IP SLAs operations are deleted for neighbors that are no longer valid.
BGP Next hop	Identifier for the BGP next hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
vrf	Name of the VPN routing or forwarding instance (VRF) that contains a routing entry for the specified BGP next hop neighbor.
Add/Delete	Indicates that the specified BGP next hop neighbor will be added to or removed from the specified VPN.

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
delete-scan-factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
mpls discovery vpn interval	Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
scan-interval	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.

show ip sla monitor mpls-lsp-monitor summary

Note Effective with Cisco IOS Release 12.2(33)SB, the **show ip sla monitor mpls-lsp-monitor summary** command is replaced by the **show ip sla mpls-lsp-monitor summary** command. See the **show ip sla mpls-lsp-monitor summary** command for more information.

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SB	This command was replaced by the **show ip sla mpls-lsp-monitor summary** command.

Usage Guidelines

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

Examples

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

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

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

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

```
4 100.1.1.4 partial 100004 19:34:07.915 EST Mon Feb 28 2005
```

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

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

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

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

Table 53 describes the significant fields shown in the display.

Table 53 show ip sla monitor mpls-lsp-monitor summary Field Descriptions

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

Related Commands

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

show ip sla monitor reaction-configuration

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor reaction-configuration** command is replaced by the **show ip sla reaction-configuration** command. See the **show ip sla reaction-configuration** command for more information.

To display the configured proactive threshold monitoring settings for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla monitor reaction-configuration** command in user EXEC or privileged EXEC mode.

show ip sla monitor reaction-configuration [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the operation for which the reaction configuration characteristics is displayed.

Defaults

Displays configured proactive threshold monitoring settings for all IP SLAs operations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla reaction-configuration** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr reaction-configuration** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla reaction-configuration** command.
12.2(33)SXI	This command was replaced by the **show ip sla reaction-configuration** command.

Usage Guidelines

Use the **ip sla monitor reaction-configuration** command in global configuration mode to configure the proactive threshold monitoring parameters for an IP SLAs operations.

Examples

In the following example, multiple monitored elements (indicated by the Reaction values) are configured for a single IP SLAs operation:

```
Router# show ip sla monitor reaction-configuration

Entry Number: 1
```

```
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None

Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly

Reaction: jitterDSAvg
Threshold type:  immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly

Reaction: PacketLossSD
Threshold type:  immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

Table 54 describes the significant fields shown in the display.

Table 54 show ip sla monitor reaction-configuration Field Descriptions

Field	Description
Reaction	The monitored element configured for the specified IP SLAs operation. Corresponds to the **react** {**connectionLoss** | **jitterAvg** | **jitterDSAvg** | **jitterSDAvg** | **mos** | **PacketLossDS** | **PacketLossSD** | **rtt** | **timeout** | **verifyError**} syntax in the **ip sla monitor reaction-configuration** command.
Threshold type	The configured threshold type. Corresponds to the **threshold-type** {**never** | **immediate** | **consecutive** | **xofy** | **average**} syntax in the **ip sla monitor reaction-configuration** command.
Rising (milliseconds)	The *upper-threshold* value. Corresponds to the **threshold-value** *upper-threshold lower-threshold* syntax in the **ip sla monitor reaction-configuration** command.
Falling (milliseconds)	The *lower-threshold* value. Corresponds to the **threshold-value** *upper-threshold lower-threshold* syntax in the **ip sla monitor reaction-configuration** command.

Table 54 show ip sla monitor reaction-configuration Field Descriptions (continued)

Field	Description
Threshold Count	The *x-value* in the **xofy** threshold type, or the *number-of-measurements* value for the **average** threshold type.
Threshold Count2	The *y-value* in the **xofy** threshold type.
Action Type	The reaction to be performed when the violation conditions are met. Corresponds to the **action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**} syntax in the **ip sla monitor reaction-configuration** command.

Related Commands

Command	Description
ip sla monitor reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.

show ip sla monitor reaction-trigger

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor reaction-trigger** command is replaced by the **show ip sla reaction-trigger** command. See the **show ip sla reaction-trigger** command for more information.

To display the reaction trigger information for all Cisco IOS IP Service Level Agreements (SLAs) operations or the specified operation, use the **show ip sla monitor reaction-trigger** command in user EXEC or privileged EXEC mode.

show ip sla monitor reaction-trigger [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla reaction-trigger** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr reaction-trigger** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla reaction-trigger** command.
12.2(33)SXI	This command was replaced by the **show ip sla reaction-trigger** command.

Usage Guidelines

Use the **show ip sla monitor reaction-trigger** command to display the configuration status and operational state of target operations that will be triggered as defined with the **ip sla monitor reaction-configuration** global configuration command.

Examples

The following is sample output from the **show ip sla monitor reaction-trigger** command:

```
Router# show ip sla monitor reaction-trigger 1

        Reaction Table
Entry Number: 1
Target Entry Number: 2
Status of Entry (SNMP RowStatus): active
Operational State: pending
```

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla monitor responder

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor responder** command is replaced by the **show ip sla responder** command. See the **show ip sla responder** command for more information.

To display information about the Cisco IOS IP Service Level Agreements (SLAs) Responder, use the **show ip sla monitor responder** command in user EXEC or privileged EXEC mode.

show ip sla monitor responder

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla responder** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr responder** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla responder** command.
12.2(33)SXI	This command was replaced by the **show ip sla responder** command.

Usage Guidelines

Use the **show ip sla monitor responder** command to display information about recent sources of IP SLAs control messages, such as who has sent recent control messages and who has sent invalid control messages.

Examples

The following is sample output from the **show ip sla monitor responder** command:

```
Router# show ip sla monitor responder

IP SLA Monitor Responder is: Enabled
Number of control message received: 19 Number of errors: 1
Recent sources:
    10.0.0.1 [19:11:49.035 UTC Sat Dec 2 1995]
    10.0.0.1 [19:10:49.023 UTC Sat Dec 2 1995]
    10.0.0.1 [19:09:48.707 UTC Sat Dec 2 1995]
    10.0.0.1 [19:08:48.687 UTC Sat Dec 2 1995]
    10.0.0.1 [19:07:48.671 UTC Sat Dec 2 1995]

Recent error sources:
    10.0.0.1 [19:10:49.023 UTC Sat Dec 2 1995] RTT_AUTH_FAIL
```

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values for IP SLAs operations.

show ip sla monitor statistics

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor statistics** command is replaced by the **show ip sla statistics** command. See the **show ip sla statistics** command for more information.

To display the current operational status and statistics of all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla monitor statistics** command in user EXEC or privileged EXEC mode.

show ip sla monitor statistics [*operation-number*] [**details**]

Syntax Description

operation-number	(Optional) Number of the operation for which operational status and statistics are displayed.
details	(Optional) Operational status and statistics are displayed in greater detail.

Defaults

Displays output for all running IP SLAs operations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla statistics** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr operational-state** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla statistics** command.
12.2(33)SXI	This command was replaced by the **show ip sla statistics** command.

Usage Guidelines

Use the **show ip sla monitor statistics** command to display the current state of IP SLAs operations, including how much life the operation has left, whether the operation is active, and the completion time. The output will also include the monitoring data returned for the last (most recently completed) operation.

Examples

The following is sample output from the **show ip sla monitor statistics** command:

```
Router# show ip sla monitor statistics

        Current Operational State
Entry Number: 3
```

```
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

The following is sample output from the **show ip sla monitor statistics** command when the specified operation is a UDP jitter (codec) operation. The values shown indicate the values for the last IP SLAs operation.

```
Router# show ip sla monitor statistics

        Current Operational State
Entry number: 10
Modification time: 12:57:45.690 UTC Sun Oct 26 2003
Number of operations attempted: 3
Number of operations skipped: 0
Current seconds left in Life: 3570
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 19
Latest operation start time: 12:57:45.723 Sun Oct 26 2003
Latest operation return code: OK
Voice Scores:
 ICPIF:  20          MOS Score:  3.20
RTT Values:
 NumOfRTT: 10     RTTAvg: 19      RTTMin: 19     RTTMax: 20
 RTTSum:  191    RTTSum2: 3649
Packet Loss Values:
 PacketLossSD: 0 PacketLossDS: 0
 PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
 InternalError: 0        Busies: 0
Jitter Values:
 NumOfJitterSamples: 9
 MinOfPositivesSD: 0     MaxOfPositivesSD: 0
 NumOfPositivesSD: 0     SumOfPositivesSD: 0     Sum2PositivesSD: 0
 MinOfNegativesSD: 0     MaxOfNegativesSD: 0
 NumOfNegativesSD: 0     SumOfNegativesSD: 0     Sum2NegativesSD: 0
 MinOfPositivesDS: 1     MaxOfPositivesDS: 1
 NumOfPositivesDS: 1     SumOfPositivesDS: 1     Sum2PositivesDS: 1
 MinOfNegativesDS: 1     MaxOfNegativesDS: 1
 NumOfNegativesDS: 1     SumOfNegativesDS: 1     Sum2NegativesDS: 1
 Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
 NumOfOW: 0
 OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
 OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0
```

Table 55 describes the significant fields shown in the display.

Table 55 show ip sla monitor statistics Field Descriptions

Field	Description
Voice Scores	Indicates that Voice over IP statistics appear on the following lines. Voice score data is computed when the operation type is configured as **type jitter** (codec).
ICPIF	The Calculated Planning Impairment Factor (ICPIF) value for the operation. The ICPIF value is computed by IP SLAs using the formula *Icpif* = *Io* + *Iq* + *Idte* + *Idd* + *Ie* – *A*, where • The values for *Io*, *Iq*, and *Idte* are set to zero. • The value *Idd* is computed based on the measured one-way delay. • The value *Ie* is computed based on the measured packet loss. • The value of A is specified by the user. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically lower than 20 are generally considered “adequate.” **Note** This value is intended only for relative comparisons, and may not match ICPIF values generated using alternate methods.
MOS Score	The estimated Mean Opinion Score (Conversational Quality, Estimated) for the latest iteration of the operation. The MOS-CQE is computed by IP SLAs as a function of the ICPIF. MOS values are expressed as a number from 1 (1.00) to 5 (5.00), with 5 being the highest level of quality, and 1 being the lowest level of quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.
RTT Values	Indicates that round-trip-time statistics appear on the following lines.
NumOfRTT	The number of successful round-trips.
RTTSum	The sum of all successful round-trip values (in milliseconds).
RTTSum2	The sum of squares of those round-trip values (in milliseconds).
PacketLossSD	The number of packets lost from source to destination.
PacketLossDS	The number of packets lost from destination to source.

Table 55 show ip sla monitor statistics Field Descriptions (continued)

Field	Description
PacketOutOfSequence	The number of packets returned out of order.
PacketMIA	The number of packets lost where the direction (SD/DS) cannot be determined.
PacketLateArrival	The number of packets that arrived after the timeout.
InternalError	The number of times an operation could not be started due to other internal failures.
Busies	The number of times this operation could not be started because the previously scheduled run was not finished.
Jitter Values:	Indicates that jitter statistics appear on the following lines. Jitter is interpacket delay variance.
NumOfJitterSamples	The number of jitter samples collected. This is the number of samples that are used to calculate the following jitter statistics.
MinOfPositivesSD MaxOfPositivesSD	The minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	The number of jitter values from source to destination that are positive (that is, network latency increases for two consecutive test packets).
SumOfPositivesSD	The sum of those positive values (in milliseconds).
Sum2PositivesSD	The sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	The minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	The number of jitter values from source to destination that are negative (that is, network latency decreases for two consecutive test packets).
SumOfNegativesSD	The sum of those values.
Sum2NegativesSD	The sum of the squares of those values.
Interarrival jitterout	The source-to-destination (SD) jitter value calculation, as defined in RFC 1889.
Interarrival jitterin	The destination-to-source (DS) jitter value calculation, as defined in RFC 1889.

Table 55 show ip sla monitor statistics Field Descriptions (continued)

Field	Description
One Way Values	Indicates that one-way measurement statistics appear on the following lines. One Way (OW) values are the amount of time required for the packet to travel from the source router to the target router (SD) or from the target router to the source router (DS).
NumOfOW	Number of successful one-way time measurements.
OWMinSD	Minimum time (in milliseconds) from the source to the destination.
OWMaxSD	Maximum time (in milliseconds) from the source to the destination.
OWSumSD	Sum of the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

Related Commands

Command	Description
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla monitor statistics aggregated

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **show ip sla monitor statistics aggregated** command is replaced by the **show ip sla statistics aggregated** command. See the **show ip sla statistics aggregated** command for more information.

To display the aggregated statistical errors and distribution information for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla monitor statistics aggregated** command in user EXEC or privileged EXEC mode.

show ip sla monitor statistics aggregated [*operation-number*] [**details**]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.
details	(Optional) Aggregated statistical information is displayed in greater detail. Distribution information is included when this keyword is specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(4)T	This command was replaced by the **show ip sla statistics aggregated** command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **show rtr collection-statistics** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **show ip sla statistics aggregated** command.
12.2(33)SXI	This command was replaced by the **show ip sla statistics aggregated** command.

Usage Guidelines

Use this command to display information such as the number of failed operations and the failure reason. The distributions statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completion times squared (used to calculate standard deviation)
- The maximum and minimum completion time
- The number of completed attempts

This command shows information collected over the past two hours, unless you specify a different amount of time using the **hours-of-statistics-kept** command.

Note This command does not support the IP SLAs ICMP path jitter operation.

Examples

The following sections show sample output from the **show ip sla monitor statistics aggregated** and **show ip sla monitor statistics aggregated details** commands for different IP SLAs operations.

Output for HTTP Operations

The following example shows output from the **show ip sla monitor statistics aggregated** and **show ip sla monitor statistics aggregated details** commands when the specified operation is a Hypertext Transfer Protocol (HTTP) operation:

```
Router# show ip sla monitor statistics aggregated 1

Round trip time (RTT) Index 3
DNS RTT: 3004 ms
TCP Connection RTT: 16 ms
HTTP Transaction RTT: 84 ms
Number of successes: 0
Number of failures: 1

Router# show ip sla monitor statistics aggregated 1 details

Round trip time (RTT) Index 3
DNS RTT: 3004
TCP Connection RTT: 0
HTTP Transaction RTT: 0
HTTP time to first byte: 0
DNS TimeOut: 0
TCP TimeOut: 0
Transaction TimeOut: 0
DNS Error: 0
TCP Error: 0
Number of successes: 0
Number of failures: 1
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/0/0/0
Failed Operations due to Internal/Sequence/Verify Error: 1/0/0
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for UDP Jitter Operations

The following is sample output from the **show ip sla monitor statistics aggregated** and **show ip sla monitor statistics aggregated details** commands when the specified operation is a User Datagram Protocol (UDP) jitter operation:

```
Router# show ip sla monitor statistics aggregated 2

Round trip time (RTT) Index 7
RTT Values
        Number Of RTT: 10
        RTT Min/Avg/Max: 1/1/2 ms
Latency one-way time milliseconds
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Latency Min/Avg/Max: 0/0/0 ms
        Destination to source Latency one way Min/Avg/Max: 0/0/0 ms
Jitter time milliseconds
        Number of Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source Jitter Min/Avg/Max: 1/1/1 ms
Packet Loss Values
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Number of successes: 1
Number of failures: 1

Router# show ip sla monitor statistics aggregated 2 details

Round trip time (RTT) Index 7
RTT Values
        Number Of RTT: 10
        RTT Min/Avg/Max: 1/1/1 ms
Latency one-way time milliseconds
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0 ms
        Destination to Source Latency one way Min/Avg/Max: 0/0/0 ms
        Source to Destination Latency one way Sum/Sum2: 0/0
        Destination to Source Latency one way Sum/Sum2: 0/0
Jitter time milliseconds
        Number of Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source Jitter Min/Avg/Max: 1/1/1 ms
        Source to destination positive jitter Min/Avg/Max: 1/1/1 ms
        Source to destination positive jitter Number/Sum/Sum2:  1/1/1
        Source to destination negative jitter Min/Avg/Max: 1/1/1 ms
        Source to destination negative jitter Number/Sum/Sum2: 1/1/1
        Destination to Source positive jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source positive jitter Number/Sum/Sum2:  2/2/2
        Destination to Source negative jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source negative jitter Number/Sum/Sum2: 2/2/2
        Interarrival jitterout: 0       Interarrival jitterin: 0
Packet Loss Values
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Number of successes: 3
Number of failures: 1
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/23/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

```
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for ICMP Echo Operations

The following is sample output from the **show ip sla monitor statistics aggregated** and **show ip sla monitor statistics aggregated details** commands when the specified operation is an Internet Control Message Protocol (ICMP) echo operation:

```
Router# show ip sla monitor statistics aggregated 3

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
RTT Values
        Number Of RTT: 0
        RTT Min/Avg/Max: 0/0/0 ms
Number of successes: 0
Number of failures: 21

Router# show ip sla monitor statistics aggregated 3 details

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
RTT Values
        Number Of RTT: 0
        RTT Min/Avg/Max: 0/0/0 ms
Number of successes: 0
Number of failures: 23
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/23/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for TCP Connect, DNS, FTP, DHCP, and UDP Echo Operations

The following is sample output from the **show ip sla monitor statistics aggregated** and **show ip sla monitor statistics aggregated details** commands when the specified operation is a Transmission Control Protocol (TCP) connect, Domain Name System (DNS), File Transfer Protocol (FTP), Dynamic Host Configuration Protocol (DHCP), or UDP echo operation:

```
Router# show ip sla monitor statistics aggregated 3

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Number of successes: 0
Number of failures: 21
```

```
Router# show ip sla monitor statistics aggregated 3 details

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Number of successes: 0
Number of failures: 23
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/23/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for ICMP Path Echo Operations

The following is sample output from the **show ip sla monitor statistics aggregated** and **show ip sla monitor statistics aggregated details** commands when the specified operation is an ICMP path echo operation:

```
Router# show ip sla monitor statistics aggregated 3

Round trip time (RTT) Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 1
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 2
Number of successes: 0
Number of failures: 21

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 3
Number of successes: 0
Number of failures: 21
.
.
```

.

```
Router# show ip sla monitor statistics aggregated 3 details

Round trip time (RTT) Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 1
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 2
Number of successes: 0
Number of failures: 21
```

```
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 3
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0-9 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10-19 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >20 ms:
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
.
.
.
```

Related Commands

Command	Description
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla monitor totals-statistics

Note Effective with Cisco IOS Release 12.4(2)T, the **show ip sla monitor totals-statistics** command is replaced by the **show ip sla monitor statistics aggregated** command. See the **show ip sla statistics aggregated** command for more information.

To display the total statistical values (accumulation of error counts and completions) for all Cisco IOS IP Service Level Agreements (SLAs) operations or the specified operation, use the **show ip sla monitor totals-statistics** command in user EXEC or privileged EXEC mode.

show ip sla monitor totals-statistics [*number*] [**tabular** | **full**]

Syntax Description

number	(Optional) Number of the IP SLAs operation to display.
tabular	(Optional) Display information in a column format, reducing the number of screens required to display the information.
full	(Optional) Display all information, using identifiers next to each displayed value. This is the default.

Defaults

Full format for all operations

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was replaced by the **show ip sla monitor statistics aggregated** command.

Usage Guidelines

The total statistics consist of the following items:

- The operation number
- The start time of the current hour of statistics
- The age of the current hour of statistics
- The number of attempted operations

You can also use the **show ip sla monitor distributions-statistics** and **show ip sla monitor collection-statistics** commands to display additional statistical information.

Examples

The following is sample output from the **show ip sla monitor totals-statistics** command in full format:

```
Router# show ip sla monitor totals-statistics
```

```
        Statistic Totals
Entry Number: 1
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Age of Statistics Entry (hundredths of seconds): 48252
Number of Initiations: 10
```

Related Commands

Command	Description
show ip sla monitor collection-statistics	Displays statistical errors for all IP SLAs operations or the specified operation.
show ip sla monitor configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show ip sla monitor distributions-statistics	Displays statistics distribution information (captured response times) for all IP SLAs operations or the specified operation.

show ip sla mpls-lsp-monitor collection-statistics

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor mpls-lsp-monitor collection-statistics** command.

Usage Guidelines

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

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

Examples

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

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

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

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

Table 56 describes the significant fields shown in the display.

Table 56 show ip sla mpls-lsp-monitor collection-statistics Field Descriptions

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

Related Commands

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

show ip sla mpls-lsp-monitor configuration

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

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

Syntax Description

operation-number	(Optional) Number of the LSP Health Monitor operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type      : echo
Vrf Name            : ipsla-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 1000
Threshold(ms)       : 5000
Frequency(sec)      : Equals schedule period
LSP Selector        : 127.0.0.1
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100001-100003
Schedule Period(sec): 60
Request size        : 100
Start Time          : Start Time already passed
```

```
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Secondary Frequency : Enabled on Timeout
         Value(sec) : 10
Reaction Configs    :
    Reaction        : connectionLoss
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
    Reaction        : timeout
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
```

Table 57 describes the significant fields shown in the display.

Table 57 show ip sla mpls-lsp-monitor configuration Field Descriptions

Field	Description
Entry Number	Identification number for the LSP Health Monitor operation.
Operation Type	Type of IP SLAs operation configured by the LSP Health Monitor operation.
Vrf Name	If a specific name is displayed in this field, then the LSP Health Monitor is configured to discover only those BGP next hop neighbors in use by the VRF specified. If ipsla-vrf-all is displayed in this field, then the LSP Health Monitor is configured to discover all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router.
Tag	User-specified identifier for an IP SLAs operation.
EXP Value	Experimental field value in the header for an echo request packet of the IP SLAs operation.
Timeout(ms)	Amount of time the IP SLAs operation waits for a response from its request packet.
Threshold(ms)	Upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Frequency(sec)	Time after which the IP SLAs operation is restarted.
LSP Selector	Local host IP address used to select the LSP for the IP SLAs operation.
ScanInterval(min)	Time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.
Delete Scan Factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
Operations List	Identification numbers of the IP SLAs operations created by the LSP Health Monitor operation.

Table 57 show ip sla mpls-lsp-monitor configuration Field Descriptions (continued)

Field	Description
Schedule Period(sec)	Time period (in seconds) in which the start times of the individual IP SLAs operations are distributed.
Request size	Protocol data size for the request packet of the IP SLAs operation.
Start Time	Status of the start time for the LSP Health Monitor operation.
SNMP RowStatus	Indicates whether SNMP RowStatus is active or inactive.
TTL value	The maximum hop count for an echo request packet of the IP SLAs operation.
Reply Mode	Reply mode for an echo request packet of the IP SLAs operation.
Reply Dscp Bits	Differentiated services codepoint (DSCP) value of an echo reply packet of the IP SLAs operation.
Secondary Frequency	Reaction condition that will enable the secondary frequency option.
Value(sec)	Secondary frequency value.
Reaction Configs	Reaction configuration of the IP SLAs operation.
Reaction	Reaction condition being monitored.
Threshold Type	Specifies when an action should be performed as a result of a reaction event.
Threshold Count	The number of times a reaction event can occur before an action should be performed.
Action Type	Type of action that should be performed as a result of a reaction event.

Related Commands

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

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

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor mpls-lsp-monitor lpd operational-state** command.

Usage Guidelines

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

Examples

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

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

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

Table 58 describes the significant fields shown in the display.

Table 58 show ip sla mpls-lsp-monitor lpd operational-state Field Descriptions

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

Related Commands

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

show ip sla mpls-lsp-monitor neighbors

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

show ip sla mpls-lsp-monitor neighbors

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr mpls-lsp-monitor neighbors** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor mpls-lsp-monitor neighbors** command.

Examples

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

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

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

Table 59 describes the significant fields shown in the display.

Table 59 show ip sla mpls-lsp-monitor neighbors Field Descriptions

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

Table 59 show ip sla mpls-lsp-monitor neighbors Field Descriptions (continued)

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

Related Commands

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

show ip sla mpls-lsp-monitor scan-queue

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

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

Syntax Description

operation-number	Number of the LSP Health Monitor operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr mpls-lsp-monitor scan-queue** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor mpls-lsp-monitor scan-queue** command.

Examples

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

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

Next scan Time after: 23 Secs
Next Delete scan Time after: 83 Secs

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

Table 60 describes the significant fields shown in the display.

Table 60 show ip sla mpls-lsp-monitor scan-queue Field Descriptions

Field	Description
Next scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about adding BGP next hop neighbors to a particular VPN. At the start of each scan time, IP SLAs operations are created for all newly discovered neighbors.
Next Delete scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about deleting BGP next hop neighbors from a particular VPN. At the start of each delete scan time, IP SLAs operations are deleted for neighbors that are no longer valid.
BGP Next hop	Identifier for the BGP next hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
vrf	Name of the VRF that contains a routing entry for the specified BGP next hop neighbor.
Add/Delete	Indicates that the specified BGP next hop neighbor will be added to or removed from the specified VPN.

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
delete-scan-factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
mpls discovery vpn interval	Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
scan-interval	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.

show ip sla mpls-lsp-monitor summary

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

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

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor mpls-lsp-monitor summary** command.

Usage Guidelines

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

Examples

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

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

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

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

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

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

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

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

Table 61 describes the significant fields shown in the display.

Table 61 show ip sla mpls-lsp-monitor summary Field Descriptions

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

Related Commands

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

show ip sla reaction-configuration

To display the configured proactive threshold monitoring settings for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla reaction-configuration** command in user EXEC or privileged EXEC mode.

show ip sla reaction-configuration [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the operation for which the reaction configuration characteristics is displayed.

Defaults

Displays configured proactive threshold monitoring settings for all IP SLAs operations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor reaction-configuration** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr reaction-configuration** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor reaction-configuration** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor reaction-configuration** command.

Usage Guidelines

Use the **ip sla reaction-configuration** command in global configuration mode to configure the proactive threshold monitoring parameters for an IP SLAs operations.

Examples

In the following example, multiple monitored elements (indicated by the Reaction values) are configured for a single IP SLAs operation:

```
Router# show ip sla reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
```

```
Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly

Reaction: jitterDSAvg
Threshold type:  immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly

Reaction: PacketLossSD
Threshold type:  immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

Table 62 describes the significant fields shown in the display.

Table 62 show ip sla reaction-configuration Field Descriptions

Field	Description
Reaction	The monitored element configured for the specified IP SLAs operation. Corresponds to the **react** {**connectionLoss** | **jitterAvg** | **jitterDSAvg** | **jitterSDAvg** | **mos** | **PacketLossDS** | **PacketLossSD** | **rtt** | **timeout** | **verifyError**} syntax in the **ip sla reaction-configuration** command.
Threshold type	The configured threshold type. Corresponds to the **threshold-type** {**never** | **immediate** | **consecutive** | **xofy** | **average**} syntax in the **ip sla reaction-configuration** command.
Rising (milliseconds)	The *upper-threshold* value. Corresponds to the **threshold-value** *upper-threshold lower-threshold* syntax in the **ip sla reaction-configuration** command.
Falling (milliseconds)	The *lower-threshold* value. Corresponds to the **threshold-value** *upper-threshold lower-threshold* syntax in the **ip sla reaction-configuration** command.
Threshold Count	The *x-value* in the **xofy** threshold type, or the *number-of-measurements* value for the **average** threshold type.

Table 62 show ip sla reaction-configuration Field Descriptions (continued)

Field	Description
Threshold Count2	The *y-value* in the **xofy** threshold type.
Action Type	The reaction to be performed when the violation conditions are met. Corresponds to the **action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**} syntax in the **ip sla reaction-configuration** command.

Related Commands

Command	Description
ip sla reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.

show ip sla reaction-trigger

To display the reaction trigger information for all Cisco IOS IP Service Level Agreements (SLAs) operations or the specified operation, use the **show ip sla reaction-trigger** command in user EXEC or privileged EXEC mode.

show ip sla reaction-trigger [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor reaction-trigger** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr reaction-trigger** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor reaction-trigger** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor reaction-trigger** command.

Usage Guidelines

Use the **show ip sla reaction-trigger** command to display the configuration status and operational state of target operations that will be triggered as defined with the **ip sla reaction-configuration** global configuration command.

Examples

The following is sample output from the **show ip sla reaction-trigger** command:

```
Router# show ip sla reaction-trigger 1

        Reaction Table
Entry Number: 1
Target Entry Number: 2
Status of Entry (SNMP RowStatus): active
Operational State: pending
```

Related Commands

Command	Description
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla responder

To display information about the Cisco IOS IP Service Level Agreements (SLAs) Responder, use the **show ip sla responder** command in user EXEC or privileged EXEC mode.

show ip sla responder

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor responder** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr responder** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor responder** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor responder** command.

Usage Guidelines

Use the **show ip sla responder** command to display information about recent sources of IP SLAs control messages, such as who has sent recent control messages and who has sent invalid control messages.

Examples

The following sections show sample output from the **show ip sla responder** command for IP SLAs Responders in IPv4 and IPv6 networks.

Output in an IPv4 Network

The following is sample output from the **show ip sla responder** command in an IPv4 network:

```
Router# show ip sla responder

IP SLA Monitor Responder is: Enabled
Number of control message received: 19 Number of errors: 1
Recent sources:
    10.0.0.1 [19:11:49.035 UTC Sat Dec 2 2005]
    10.0.0.1 [19:10:49.023 UTC Sat Dec 2 2005]
    10.0.0.1 [19:09:48.707 UTC Sat Dec 2 2005]
    10.0.0.1 [19:08:48.687 UTC Sat Dec 2 2005]
    10.0.0.1 [19:07:48.671 UTC Sat Dec 2 2005]

Recent error sources:
    10.0.0.1 [19:10:49.023 UTC Sat Dec 2 2005] RTT_AUTH_FAIL
```

Output in an IPv6 Network

The following is sample output from the **show ip sla responder** command in an IPv6 network:

```
Router# show ip sla responder

IP SLA Responder is: Enabled
Number of control message received: 19 Number of errors: 1
Recent sources:
    2001:DB8:100::1 [19:11:49.035 IST Thu Jul 13 2006]
    2001:DB8:100::1 [19:10:49.023 IST Thu Jul 13 2006]
    2001:DB8:100::1 [19:09:48.707 IST Thu Jul 13 2006]
    2001:DB8:100::1 [19:08:48.687 IST Thu Jul 13 2006]
    2001:DB8:100::1 [19:07:48.671 IST Thu Jul 13 2006]

Recent error sources:
    2001:DB8:100::1 [19:10:49.023 IST Thu Jul 13 2006] RTT_AUTH_FAIL
```

Related Commands

Command	Description
show ip sla configuration	Displays configuration values for IP SLAs operations.

show ip sla statistics

To display the current operational status and statistics of all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla statistics** command in user EXEC or privileged EXEC mode.

show ip sla statistics [*operation-number*] [**details**]

Syntax Description

operation-number	(Optional) Number of the operation for which operational status and statistics are displayed.
details	(Optional) Operational status and statistics are displayed in greater detail.

Defaults

Displays output for all running IP SLAs operations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor statistics** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr operational-state** command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor statistics** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor statistics** command.

Usage Guidelines

Use the **show ip sla statistics** command to display the current state of IP SLAs operations, including how much life the operation has left, whether the operation is active, and the completion time. The output will also include the monitoring data returned for the last (most recently completed) operation.

Examples

The following is sample output from the **show ip sla statistics** command:

```
Router# show ip sla statistics

        Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
```

```
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

The following is sample output from the **show ip sla statistics** command when the specified operation is a UDP jitter (codec) operation. The values shown indicate the values for the last IP SLAs operation.

```
Router# show ip sla statistics

        Current Operational State
Entry number: 10
Modification time: 12:57:45.690 UTC Sun Oct 26 2003
Number of operations attempted: 3
Number of operations skipped: 0
Current seconds left in Life: 3570
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 19
Latest operation start time: 12:57:45.723 Sun Oct 26 2003
Latest operation return code: OK
Voice Scores:
 ICPIF:  20          MOS Score:  3.20
RTT Values:
 NumOfRTT: 10     RTTAvg: 19      RTTMin: 19     RTTMax: 20
 RTTSum:  191    RTTSum2: 3649
Packet Loss Values:
 PacketLossSD: 0 PacketLossDS: 0
 PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
 InternalError: 0        Busies: 0
Jitter Values:
 NumOfJitterSamples: 9
 MinOfPositivesSD: 0     MaxOfPositivesSD: 0
 NumOfPositivesSD: 0     SumOfPositivesSD: 0     Sum2PositivesSD: 0
 MinOfNegativesSD: 0     MaxOfNegativesSD: 0
 NumOfNegativesSD: 0     SumOfNegativesSD: 0     Sum2NegativesSD: 0
 MinOfPositivesDS: 1     MaxOfPositivesDS: 1
 NumOfPositivesDS: 1     SumOfPositivesDS: 1     Sum2PositivesDS: 1
 MinOfNegativesDS: 1     MaxOfNegativesDS: 1
 NumOfNegativesDS: 1     SumOfNegativesDS: 1     Sum2NegativesDS: 1
 Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
 NumOfOW: 0
 OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
 OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0
```

Table 63 describes the significant fields shown in the display.

Table 63 show ip sla statistics Field Descriptions

Field	Description
Voice Scores	Indicates that Voice over IP statistics appear on the following lines. Voice score data is computed when the operation type is configured as **udp-jitter** (codec).
ICPIF	The Calculated Planning Impairment Factor (ICPIF) value for the operation. The ICPIF value is computed by IP SLAs using the formula *Icpif = Io + Iq + Idte + Idd + Ie – A*, where • The values for *Io*, *Iq*, and *Idte* are set to zero. • The value *Idd* is computed based on the measured one-way delay. • The value *Ie* is computed based on the measured packet loss. • The value of A is specified by the user. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically lower than 20 are generally considered "adequate." **Note** This value is intended only for relative comparisons, and may not match ICPIF values generated using alternate methods.
MOS Score	The estimated Mean Opinion Score (Conversational Quality, Estimated) for the latest iteration of the operation. The MOS-CQE is computed by IP SLAs as a function of the ICPIF. MOS values are expressed as a number from 1 (1.00) to 5 (5.00), with 5 being the highest level of quality, and 1 being the lowest level of quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.
RTT Values	Indicates that round-trip-time statistics appear on the following lines.
NumOfRTT	The number of successful round-trips.
RTTSum	The sum of all successful round-trip values (in milliseconds).
RTTSum2	The sum of squares of those round-trip values (in milliseconds).
PacketLossSD	The number of packets lost from source to destination.
PacketLossDS	The number of packets lost from destination to source.
PacketOutOfSequence	The number of packets returned out of order.

Table 63 show ip sla statistics Field Descriptions (continued)

Field	Description
PacketMIA	The number of packets lost where the direction (SD/DS) cannot be determined.
PacketLateArrival	The number of packets that arrived after the timeout.
InternalError	The number of times an operation could not be started due to other internal failures.
Busies	The number of times this operation could not be started because the previously scheduled run was not finished.
Jitter Values	Indicates that jitter statistics appear on the following lines. Jitter is interpacket delay variance.
NumOfJitterSamples	The number of jitter samples collected. This is the number of samples that are used to calculate the following jitter statistics.
MinOfPositivesSD MaxOfPositivesSD	The minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	The number of jitter values from source to destination that are positive (that is, network latency increases for two consecutive test packets).
SumOfPositivesSD	The sum of those positive values (in milliseconds).
Sum2PositivesSD	The sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	The minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	The number of jitter values from source to destination that are negative (that is, network latency decreases for two consecutive test packets).
SumOfNegativesSD	The sum of those values.
Sum2NegativesSD	The sum of the squares of those values.
Interarrival jitterout	The source-to-destination (SD) jitter value calculation, as defined in RFC 1889.
Interarrival jitterin	The destination-to-source (DS) jitter value calculation, as defined in RFC 1889.
One Way Values	Indicates that one-way measurement statistics appear on the following lines. One Way (OW) values are the amount of time required for the packet to travel from the source router to the target router (SD) or from the target router to the source router (DS).

Table 63 show ip sla statistics Field Descriptions (continued)

Field	Description
NumOfOW	Number of successful one-way time measurements.
OWMinSD	Minimum time (in milliseconds) from the source to the destination.
OWMaxSD	Maximum time (in milliseconds) from the source to the destination.
OWSumSD	Sum of the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

Related Commands

Command	Description
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show ip sla statistics aggregated

To display the aggregated statistical errors and distribution information for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show ip sla statistics aggregated** command in user EXEC or privileged EXEC mode.

show ip sla statistics aggregated [*operation-number*] [**details**]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.
details	(Optional) Aggregated statistical information is displayed in greater detail. Distribution information is included when this keyword is specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **show ip sla monitor statistics aggregated** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **show rtr collection-statistics**, **show rtr distributions-statistics**, and **show rtr totals-statistics** commands.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **show ip sla monitor statistics aggregated** command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **show ip sla monitor statistics aggregated** command.

Usage Guidelines

Use this command to display information such as the number of failed operations and the failure reason. The distributions statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completions times squared (used to calculate standard deviation)
- The maximum and minimum completion time
- The number of completed attempts

This command shows information collected over the past two hours, unless you specify a different amount of time using the **history hours-of-statistics-kept** command.

Note This command does not support the IP SLAs ICMP path jitter operation.

Examples

The following sections show sample output from the **show ip sla statistics aggregated** and **show ip sla statistics aggregated details** commands for different IP SLAs operations:

Output for HTTP Operations

The following example shows output from the **show ip sla statistics aggregated** and **show ip sla statistics aggregated details** commands when the specified operation is a Hypertext Transfer Protocol (HTTP) operation:

```
Router# show ip sla statistics aggregated 1

Round trip time (RTT) Index 3
DNS RTT: 3004 ms
TCP Connection RTT: 16 ms
HTTP Transaction RTT: 84 ms
Number of successes: 0
Number of failures: 1

Router# show ip sla statistics aggregated 1 details

Round trip time (RTT) Index 3
DNS RTT: 3004
TCP Connection RTT: 0
HTTP Transaction RTT: 0
HTTP time to first byte: 0
DNS TimeOut: 0
TCP TimeOut: 0
Transaction TimeOut: 0
DNS Error: 0
TCP Error: 0
Number of successes: 0
Number of failures: 1
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/0/0/0
Failed Operations due to Internal/Sequence/Verify Error: 1/0/0
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for UDP Jitter Operations

The following is sample output from the **show ip sla statistics aggregated** and **show ip sla statistics aggregated details** commands when the specified operation is a User Datagram Protocol (UDP) jitter operation:

```
Router# show ip sla statistics aggregated 2

Round trip time (RTT) Index 7
RTT Values
        Number Of RTT: 10
```

```
        RTT Min/Avg/Max: 1/1/2 ms
Latency one-way time milliseconds
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Latency Min/Avg/Max: 0/0/0 ms
        Destination to source Latency one way Min/Avg/Max: 0/0/0 ms
Jitter time milliseconds
        Number of Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source Jitter Min/Avg/Max: 1/1/1 ms
Packet Loss Values
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Number of successes: 1
Number of failures: 1

Router# show ip sla statistics aggregated 2 details

Round trip time (RTT) Index 7
RTT Values
        Number Of RTT: 10
        RTT Min/Avg/Max: 1/1/1 ms
Latency one-way time milliseconds
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0 ms
        Destination to Source Latency one way Min/Avg/Max: 0/0/0 ms
        Source to Destination Latency one way Sum/Sum2: 0/0
        Destination to Source Latency one way Sum/Sum2: 0/0
Jitter time milliseconds
        Number of Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source Jitter Min/Avg/Max: 1/1/1 ms
        Source to destination positive jitter Min/Avg/Max: 1/1/1 ms
        Source to destination positive jitter Number/Sum/Sum2:  1/1/1
        Source to destination negative jitter Min/Avg/Max: 1/1/1 ms
        Source to destination negative jitter Number/Sum/Sum2: 1/1/1
        Destination to Source positive jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source positive jitter Number/Sum/Sum2:  2/2/2
        Destination to Source negative jitter Min/Avg/Max: 1/1/1 ms
        Destination to Source negative jitter Number/Sum/Sum2: 2/2/2
        Interarrival jitterout: 0       Interarrival jitterin: 0
Packet Loss Values
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Number of successes: 3
Number of failures: 1
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/23/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for ICMP Echo Operations

The following is sample output from the **show ip sla statistics aggregated** and **show ip sla statistics aggregated details** commands when the specified operation is an Internet Control Message Protocol (ICMP) echo operation:

```
Router# show ip sla statistics aggregated 3

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
RTT Values
        Number Of RTT: 0
        RTT Min/Avg/Max: 0/0/0 ms
Number of successes: 0
Number of failures: 21

Router# show ip sla statistics aggregated 3 details

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
RTT Values
        Number Of RTT: 0
        RTT Min/Avg/Max: 0/0/0 ms
Number of successes: 0
Number of failures: 23
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/23/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for TCP Connect, DNS, FTP, DHCP, and UDP Echo Operations

The following is sample output from the **show ip sla statistics aggregated** and **show ip sla statistics aggregated details** commands when the specified operation is a Transmission Control Protocol (TCP) connect, Domain Name System (DNS), File Transfer Protocol (FTP), Dynamic Host Configuration Protocol (DHCP), or UDP echo operation:

```
Router# show ip sla statistics aggregated 3

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Number of successes: 0
Number of failures: 21

Router# show ip sla statistics aggregated 3 details

Round trip time (RTT)Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Number of successes: 0
```

```
Number of failures: 23
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/23/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
```

Output for ICMP Path Echo Operations

The following is sample output from the **show ip sla statistics aggregated** and **show ip sla statistics aggregated details** commands when the specified operation is an ICMP path echo operation:

```
Router# show ip sla statistics aggregated 3

Round trip time (RTT) Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 1
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 2
Number of successes: 0
Number of failures: 21

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.896 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 3
Number of successes: 0
Number of failures: 21
.
.
.

Router# show ip sla statistics aggregated 3 details

Round trip time (RTT) Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 1
```

```
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 1
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 2
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
```

```
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0

Round trip time (RTT)   Index 3
Start Time Index: 05:31:12.897 PST Wed Sep 3 2003
Path Index: 2
Hop in Path Index: 3
Number of successes: 0
Number of failures: 21
Failed Operations due to over threshold: 0
Failed Operations due to Disconnect/TimeOut/Busy/No Connection: 0/21/0/0
Failed Operations due to Internal/Sequence/Verify Error: 0/0/0
Target Address: 10.4.23.44
Distribution Statistics:
Bucket Range: 0 to < 9ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: 10 to < 19ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
Bucket Range: >=20 ms
   Avg. Latency: 0 ms
   Percent of Total Completions for this range: 0%
   Number of Completions/Sum of Latency: 0/0/0
Sum of RTT squared low 32 Bits/ Sum of RTT squared high 32 Bits: 0/0
.
.
.
```

Related Commands

Command	Description
history hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show mpls discovery vpn

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

show mpls discovery vpn

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

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

```
Router# show mpls discovery vpn

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

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

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

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

Table 64 describes the fields shown in the display.

Table 64 show mpls discovery vpn Field Descriptions

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

Table 64 show mpls discovery vpn Field Descriptions (continued)

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

Related Commands

Command	Description
mpls discovery vpn interval	Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
mpls discovery vpn next-hop	Enables the MPLS VPN BGP next hop neighbor discovery process.

show rtr application

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

To display global information about Cisco IOS IP Service Level Agreements (IP SLAs), use the **show rtr application** command in user EXEC or privileged EXEC mode.

show rtr application [**tabular** | **full**]

Syntax Description

tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information.
full	(Optional) Displays all information using identifiers next to each displayed value. This is the default.

Defaults

Full format

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Use the **show rtr application** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show rtr application** command in full format:

```
Router# show rtr application

        SA Agent
Version: 2.2.0 Round Trip Time MIB
Time of last change in whole RTR: *17:21:30.819 UTC Tue Mar 19 2002
Estimated system max number of entries: 4699
```

```
Number of Entries configured:5
    Number of active Entries:5
   Number of pending Entries:0
  Number of inactive Entries:0
         Supported Operation Types
Type of Operation to Perform:  echo
Type of Operation to Perform:  pathEcho
Type of Operation to Perform:  udpEcho
Type of Operation to Perform:  tcpConnect
Type of Operation to Perform:  http
Type of Operation to Perform:  dns
Type of Operation to Perform:  jitter
Type of Operation to Perform:  dlsw
Type of Operation to Perform:  dhcp
Type of Operation to Perform:  ftp

        Supported Protocols
Protocol Type: ipIcmpEcho
Protocol Type: ipUdpEchoAppl
Protocol Type: snaRUEcho
Protocol Type: snaLU0EchoAppl
Protocol Type: snaLU2EchoAppl
Protocol Type: ipTcpConn
Protocol Type: httpAppl
Protocol Type: dnsAppl
Protocol Type: jitterAppl
Protocol Type: dlsw
Protocol Type: dhcp
Protocol Type: ftpAppl

Number of configurable probe is 490
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show rtr authentication

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

To display Cisco IOS IP Service Level Agreements (IP SLAs) authentication information, use the **show rtr authentication** command in user EXEC or privileged EXEC mode.

show rtr authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Use the **show rtr authentication** command to display information such as supported operation types and supported protocols.

Examples

The following is sample output from the **show rtr authentication** command:

```
Router# show rtr authentication

RTR control message uses MD5 authentication, key chain name is: rtr
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values for IP SLAs operations.

show rtr collection-statistics

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

To display statistical errors for all Cisco IOS IP Service Level Agreements (IP SLAs) operations or a specified operation, use the **show rtr collection-statistics** command in user EXEC or privileged EXEC mode.

show rtr collection-statistics [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.

Defaults

Shows statistics for the past two hours.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The output for this command was expanded to show information for Jitter operations.
12.1	The **tabular** and **full** keywords were removed.
12.1(1)T	The output for this command was expanded to show information for the FTP operation type and for One Way Delay Jitter operations.
12.2(8)T, 12.2(8)S	Output for “NumOfJitterSamples” was added (CSCdv30022).
12.2(11)T	The SAA Engine II was implemented. The maximum number of operations was increased from 500 to 2000.
12.3(4)T	Output (MOS and ICPIF scores) for the Jitter (codec) operation type was added.
12.3(7)T	Decimal granularity for MOS scores was added.
12.3(14)T	This command was replaced by the **show ip sla monitor collection-statistics** command.

Release	Modification
12.2(31)SB2	This command was replaced by the **show ip sla monitor statistics aggregated** command.
12.2(33)SRB	This command was replaced by the **show ip sla statistics aggregated** command.

Usage Guidelines

Use the **show rtr collection-statistics** command to display information such as the number of failed operations and the failure reason. You can also use the **show rtr distribution-statistics** and **show rtr totals-statistics** commands to display additional statistical information.

This command shows information collected over the past two hours, unless you specify a different amount of time using the **hours-of-statistics-kept** command.

For One Way Delay Jitter operations, the clocks on each device must be synchronized using NTP (or GPS systems). If the clocks are not synchronized, one way measurements are discarded. (If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round trip time, the one way measurement values are assumed to be faulty, and are discarded.)

Note This command does not support the IP SLAs ICMP path jitter operation.

Examples

The following shows sample output from the **show rtr collection-statistics** command in full format.

```
Router# show rtr collection-statistics 1

        Collected Statistics
Entry Number: 1
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Path Index: 1
Hop in Path Index: 1
Number of Failed Operations due to a Disconnect: 0
Number of Failed Operations due to a Timeout: 0
Number of Failed Operations due to a Busy: 0
Number of Failed Operations due to a No Connection: 0
Number of Failed Operations due to an Internal Error: 0
Number of Failed Operations due to a Sequence Error: 0
Number of Failed Operations due to a Verify Error: 0
Target Address: 172.16.1.176
```

Output for HTTP Operations

The following example shows output from the show rtr collection-statistics command when the specified operation is an HTTP operation:

```
Router# show rtr collection-statistics 2

        Collected Statistics

Entry Number:2
HTTP URL:http://172.20.150.200
Start Time:*00:01:16.000 UTC Mon Nov 1 2003

             Comps:1              RTTMin:343
             OvrTh:0              RTTMax:343
        DNSTimeOut:0              RTTSum:343
```

```
        TCPTimeOut:0              RTTSum2:117649
        TraTimeOut:0               DNSRTT:0
          DNSError:0             TCPConRTT:13
         HTTPError:0              TransRTT:330
          IntError:0              MesgSize:1771
            Busies:0
```

Output for Jitter Operations

The following is sample output from the **show rtr collection-statistics** command, where operation 2 is a Jitter operation that includes One Way statistics:

```
Router# show rtr collection-statistics

Collected Statistics

Entry Number: 2
Target Address: 5.0.0.1, Port Number:99
Start Time: 11:12:03.000 UTC Thu Jul 1 1999
RTT Values:
NumOfRTT: 600  RTTSum: 3789  RTTSum2: 138665
Packet Loss Values:
PacketLossSD: 0  PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
InternalError: 0  Busies: 0
Jitter Values:
MinOfPositivesSD: 1   MaxOfPositivesSD: 2
NumOfPositivesSD: 26  SumOfPositivesSD: 31   Sum2PositivesSD: 41
MinOfNegativesSD: 1   MaxOfNegativesSD: 4
NumOfNegativesSD: 56  SumOfNegativesSD: 73   Sum2NegativesSD: 133
MinOfPositivesDS: 1   MaxOfPositivesDS: 338
NumOfPositivesDS: 58  SumOfPositivesDS: 409  Sum2PositivesDS: 114347
MinOfNegativesDS: 1   MaxOfNegativesDS: 338
NumOfNegativesDS: 48  SumOfNegativesDS: 396  Sum2NegativesDS: 114332
One Way Values:
NumOfOW: 440
OWMinSD: 2  OWMaxSD: 6    OWSumSD: 1273  OWSum2SD: 4021
OWMinDS: 2  OWMaxDS: 341  OWSumDS: 1643  OWSum2DS: 120295
```

The values shown indicate the aggregated values for the current hour. RTT stands for Round-Trip-Time. SD stands for Source-to-Destination. DS stands for Destination-to-Source. OW stands for One Way. Table 65 describes the significant fields shown in this output.

Output for Jitter (codec) Operations

The following is sample output from the **show rtr collection-statistics** command, where operation 10 is a Jitter (codec) operation:

```
Router# show rtr collection-statistics 10
Entry number: 10
Start Time Index: 13:18:49.904 PST Mon Jun 24 2002
Number of successful operations: 2
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
Voice Scores:
MinOfICPIF: 0   MaxOfICPIF: 0   MinOfMOS: 0     MaxOfMOS: 0
RTT Values:
```

```
NumOfRTT: 122   RTTAvg: 2       RTTMin: 2       RTTMax: 3
RTTSum: 247     RTTSum2: 503
Packet Loss Values:
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0       PacketSkipped: 78  <<<<<============
Jitter Values:
MinOfPositivesSD: 1     MaxOfPositivesSD: 1
NumOfPositivesSD: 9     SumOfPositivesSD: 9     Sum2PositivesSD: 9
MinOfNegativesSD: 1     MaxOfNegativesSD: 1
NumOfNegativesSD: 8     SumOfNegativesSD: 8     Sum2NegativesSD: 8
MinOfPositivesDS: 1     MaxOfPositivesDS: 1
NumOfPositivesDS: 6     SumOfPositivesDS: 6     Sum2PositivesDS: 6
MinOfNegativesDS: 1     MaxOfNegativesDS: 1
NumOfNegativesDS: 7     SumOfNegativesDS: 7     Sum2NegativesDS: 7
Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
NumOfOW: 0
OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0
```

Table 65 show rtr collection-statistics Field Descriptions

Field	Description
Voice Scores:	Indicates that Voice over IP statistics appear on the following lines. Voice score data is computed when the operation type is configured as **type jitter (codec)**.
ICPIF	The Calculated Planning Impairment Factor (ICPIF) value for the operation. The ICPIF value is computed by IP SLAs using the formula *Icpif = Io + Iq + Idte + Idd + Ie – A*, where • the values for *Io*, *Iq*, and *Idte* are set to zero, • the value *Idd* is computed based on the measured one way delay, • the value *Ie* is computed based on the measured packet loss, • and the value of A is specified by the user. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically less than 20 are generally considered “adequate.” **Note** This value is intended only for relative comparisons, and may not match ICPIF values generated using alternate methods.
MinOfICPIF:	The lowest (minimum) ICPIF value computed for the collected statistics.
MaxOfICPIF:	The highest (maximum) ICPIF value computed for the collected statistics.
Mos	The estimated Mean Opinion Score (Conversational Quality, Estimated) for the latest iteration of the operation. The MOS-CQE is computed by IP SLAs as a function of the ICPIF. MOS values are expressed as a number from 1 (1.00) to 5 (5.00), with 5 being the highest level of quality, and 1 being the lowest level of quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.

Table 65 show rtr collection-statistics Field Descriptions (continued)

Field	Description
MinOfMos:	The lowest (minimum) MOS value computed for the collected statistics.
MaxOfMos:	The highest (maximum) ICPIF value computed for the collected statistics.
RTT Values:	Indicates that Round-Trip-Time statistics appear on the following lines.
NumOfRTT	The number of successful round trips.
RTTSum	The sum of all successful round trip values (in milliseconds).
RTTSum2	The sum of squares of those round trip values (in milliseconds).
PacketLossSD	The number of packets lost from source to destination.
PacketLossDS	The number of packets lost from destination to source.
PacketOutOfSequence	The number of packets returned out of order.
PacketMIA	The number of packets lost where the direction (SD/DS) cannot be determined.
PacketLateArrival	The number of packets that arrived after the timeout.
PacketSkipped	The number of packets that are not sent during the IP SLAs jitter operation.
InternalError	The number of times an operation could not be started due to other internal failures.
Busies	The number of times this operation could not be started because the previously scheduled run was not finished.
Jitter Values:	Indicates that Jitter statistics appear on the following lines. Jitter is inter-packet delay variance.
NumOfJitterSamples:	The number of jitter samples collected. This is the number of samples that are used to calculate the following jitter statistics.
MinOfPositivesSD MaxOfPositivesSD	The minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	The number of jitter values from source to destination that are positive (i.e., network latency increases for two consecutive test packets).
SumOfPositivesSD	The sum of those positive values (in milliseconds).
Sum2PositivesSD	The sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	The minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	The number of jitter values from source to destination that are negative (i.e., network latency decreases for two consecutive test packets).

Table 65 show rtr collection-statistics Field Descriptions (continued)

Field	Description
SumOfNegativesSD	The sum of those values.
Sum2NegativesSD	The sum of the squares of those values.
Interarrival jitterout:	The source to destination (SD) jitter value calculation, as defined in RFC 1889.
Interarrival jitterin:	The destination to source (DS) jitter value calculation, as defined in RFC 1889.
One Way Values	Indicates that one way measurement statistics appear on the following lines. One Way (OW) Values are the amount of time it took the packet to travel from the source router to the target router (SD) or from the target router to the source router (DS).
NumOfOW	Number of successful one way time measurements.
OWMinSD	Minimum time from the source to the destination.
OWMaxSD	Maximum time from the source to the destination.
OWSumSD	Sum of the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

The DS values show the same information as above for Destination-to-Source Jitter values.

Related Commands

Command	Description
show ntp status	Displays the status of the Network Time Protocol configuration on your system.
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all IP SLAs operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all IP SLAs operations or the specified operation.

show rtr configuration

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

To display configuration values including all defaults for all Cisco IOS IP Service Level Agreements (IP SLAs) operations or the specified operation, use the **show rtr configuration** command in user EXEC or privileged EXEC mode.

show rtr configuration [*operation*]

Syntax Description

operation	(Optional) Number of the IP SLAs operation for, which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1	The **tabular** and **full** keywords were removed.
12.3(2)T	Output was added to show the VRF assignment name (if configured).
12.3(4)T	Output specific to the jitter (codec) operation type was added.
12.3(7)T	Output pertaining to reaction configuration (threshold values, reaction types) was removed from the output. Reaction configuration is now displayed using the **show rtr reaction-configuration** command.
12.3(8)T	Output was added to show the group schedule and the recurring schedule details for the IP SLAs operations.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. This integration includes the addition of output to show the group schedule and recurring schedule details for the IP SLAs operations.
12.3(14)T	This command was replaced by the **show ip sla monitor configuration** command.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC. This integration includes the addition of output to show the group schedule and recurring schedule details for the IP SLAs operations.
12.2(31)SB2	This command was replaced by the **show ip sla monitor configuration** command.
12.2(33)SRB	This command was replaced by the **show ip sla configuration** command.

Examples

The following is sample output from the **show rtr configuration** command for an IP SLAs Echo operation:

```
Router# show rtr configuration

        Complete Configuration Table (includes defaults)
Entry Number: 1
Owner: "Sample Owner"
Tag: "Sample Tag Group"
Type of Operation to Perform: echo
Reaction and History Threshold (milliseconds): 5000
Operation Frequency (seconds): 60
Operation Timeout (milliseconds): 5000
Verify Data: FALSE
Status of Entry (SNMP RowStatus): active
Protocol Type: ipIcmpEcho
Target Address: 172.16.1.176
Request Size (ARR data portion): 1
Response Size (ARR data portion): 1
Life (seconds): 3600
Next Start Time: Start Time already passed
Entry Ageout (seconds): 3600

Number of Statistic Hours kept: 2
Number of Statistic Paths kept: 1
Number of Statistic Hops kept: 1
Number of Statistic Distribution Buckets kept: 1
Number of Statistic Distribution Intervals (milliseconds): 20
Number of History Lives kept: 0
Number of History Buckets kept: 50
Number of History Samples kept: 1
History Filter Type: none
```

The following is sample output from the **show rtr configuration** command that verifies the configuration of an IP SLAs HTTP operation:

```
Router# show rtr configuration

        Complete Configuration Table (includes defaults)
Entry Number:3
Owner:Joe
Tag:AppleTree
Type of Operation to Perform:http
Reaction and History Threshold (milliseconds):5000
Operation Frequency (seconds):60
Operation Timeout (milliseconds):5000
Verify Data:FALSE
Status of Entry (SNMP RowStatus):active
Protocol Type:httpAppl
Target Address:
Source Address:0.0.0.0
Target Port:0
Source Port:0
Request Size (ARR data portion):1
Response Size (ARR data portion):1
Control Packets:enabled
Loose Source Routing:disabled
LSR Path:
Type of Service Parameters:0x0
HTTP Operation:get
HTTP Server Version:1.0
URL:http://www.cisco.com
Cache Control:enabled
```

```
Life (seconds):3600
Next Scheduled Start Time:Start Time already passed
Entry Ageout:never

Number of Statistic Hours kept:2
Number of Statistic Paths kept:1
Number of Statistic Hops kept:1
Number of Statistic Distribution Buckets kept:1
Statistic Distribution Interval (milliseconds):20
Number of History Lives kept:0
Number of History Buckets kept:15
Number of History Samples kept:1
History Filter Type:none
```

The following is sample output from the **show rtr configuration** command that shows output for a PathJitter operation associated with the VPN vrf1:

```
Router# show rtr configuration 1

Entry number: 1
Owner:
Tag:
Type of operation to perform: pathJitter
Destination address: 171.69.1.129
Source address: 0.0.0.0
Number of packets: 10
Interval (milliseconds): 20
Target Only: Disabled
Request size (ARR data portion): 1
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Loose Source Routing: Disabled
Vrf Name: vrf1
LSR Path:
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 2000
Entry Ageout (seconds): never
Status of entry (SNMP RowStatus): Active
```

The following is sample output from the **show rtr configuration** command that includes output for the **type jitter (codec)** operation for VoIP metric monitoring:

```
Router# show rtr configuration

Entry number: 10
Owner: admin_bofh
Tag:
Type of operation to perform: jitter
Target address: 209.165.200.225
Source address: 0.0.0.0
Target port: 16384
Source port: 0
Operation timeout (milliseconds): 5000
Codec Type: g711alaw
Codec Number Of Packets: 1000
Codec Packet Size: 172
Codec Interval (milliseconds): 20
Advantage Factor: 2
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
```

```
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Life (seconds): 3600
Entry Ageout (seconds): never
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
```

The following is sample output from the **show rtr configuration** command for a recurring IP SLAs operation, with the recurring state as TRUE:

```
Router# show rtr configuration

Entry number: 5
Owner:
Tag:
Type of operation to perform: udpEcho
Target address: 10.2.31.121
Source address: 0.0.0.0
Target port: 989
Source port: 0
Request size (ARR data portion): 16
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled: FALSE
Group Schedule Entry number :
Life (seconds): 3600
Entry Ageout (seconds): never
Recurring (Starting everyday): TRUE
Status of entry (SNMP RowStatus): Active
Connection loss reaction enabled: No
```

Related Commands

Command	Description
show rtr application	Displays global information about the IP SLAs feature.
show rtr collection-statistics	Displays statistical errors for all IP SLAs operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all IP SLAs operations or the specified operation.
show rtr group schedule	Displays the group schedule details of the specified IP SLAs operation.
show rtr history	Displays history collected for all IP SLAs operations or the specified operation.
show rtr operational-state	Displays the operational state of all IP SLAs operations or the specified operation.

Command	Description
show rtr reaction-trigger	Displays the reaction trigger information for all IP SLAs operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all IP SLAs operations or the specified operation.

show rtr distributions-statistics

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

To display statistic distribution information (captured response times) for all Cisco IOS IP Service Level Agreements (IP SLAs) operations or the specified operation, use the **show rtr distributions-statistics** command in user EXEC or privileged EXEC mode.

show rtr distributions-statistics [*operation*] [**tabular** | **full**]

Syntax Description

operation	(Optional) Number of the IP SLAs operation to display.
tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information using identifiers next to each displayed value.

Defaults

Tabular format for all operations is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the **show ip sla monitor distributions-statistics** command.
12.2(31)SB2	This command was replaced by the **show ip sla monitor statistics aggregated** command.
12.2(33)SRB	This command was replaced by the **show ip sla statistics aggregated** command.

Usage Guidelines

The distributions statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completions times squared (used to calculate standard deviation)
- The maximum and minimum completion time

- The number of completed attempts

Note This command does not support the IP SLAs ICMP path jitter operation.

You can also use the **show rtr collection-statistics** and **show rtr totals-statistics** commands to display additional statistical information.

Examples

The following is sample output from the **show rtr distributions-statistics** command in tabular format when the output is split over multiple lines

```
Router# show rtr distributions-statistics

        Captured Statistics
        Multiple Lines per Entry
Line 1
Entry    = Entry Number
StartT   = Start Time of Entry (hundredths of seconds)
Pth      = Path Index
Hop      = Hop in Path Index
Dst      = Time Distribution Index
Comps    = Operations Completed
OvrTh    = Operations Completed Over Thresholds
SumCmp   = Sum of Completion Times (milliseconds)
Line 2
SumCmp2L = Sum of Completion Times Squared Low 32 Bits (milliseconds)
SumCmp2H = Sum of Completion Times Squared High 32 Bits (milliseconds)
TMax     = Completion Time Maximum (milliseconds)
TMin     = Completion Time Minimum (milliseconds)
Entry StartT     Pth Hop Dst Comps      OvrTh      SumCmp
  SumCmp2L   SumCmp2H   TMax       TMin
1     17417068   1   1   1   2          0           128
   8192      0          64         64
```

The following example shows the output as it appears on a single line:

```
Entry StartT   Pth Hop Dst Comps  OvrTh   SumCmp    SumCmp2L   SumCmp2H  TMax     TMin
10    3581     1   1   1   0      0       0         0          0         0        0
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all IP SLAs operations or the specified operation.
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all IP SLAs operations or the specified operation.

show rtr enhanced-history collection-statistics

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

To display enhanced history statistics for all collected history buckets for the specified Cisco IOS IP Service Level Agreements (IP SLAs) operation, use the **show rtr enhanced-history collection-statistics** command in user EXEC or privileged EXEC mode.

show rtr enhanced-history collection-statistics [*operation-number*] [**interval** *seconds*]

Syntax Description

operation-number	(Optional) Displays enhanced history distribution statistics for only the specified operation.
interval *seconds*	(Optional) Displays enhanced history distribution statistics for only the specified aggregation interval.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(14)T	This command was replaced by the **show ip sla monitor enhanced-history collection-statistics** 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 **show ip sla monitor enhanced-history collection-statistics** command.
12.2(33)SRB	This command was replaced by the **show ip sla enhanced-history collection-statistics** command.

Usage Guidelines

This command displays data for each bucket of enhanced history data shown individually (one after the other).

The number of buckets and the collection interval is set using the **enhanced-history interval** *seconds* **buckets** *number-of-buckets* RTR configuration command.

Examples

The following example shows sample output for the **show rtr enhanced-history collection-statistics** command. The output of this command will vary depending on the type of IP SLAs operation.

```
Router# show rtr enhanced-history collection-statistics 1
Entry number: 1
Aggregation Interval: 900

Bucket Index: 1
Aggregation start time 00:15:00.003 UTC Thur May 1 2003
Target Address:
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 0
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 0
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
 .
 .
 .
```

Table 66 describes the significant fields shown in the display.

Table 66 show rtr enhanced-history collection-statistics Field Descriptions

Field	Description
Aggregation Interval:	The number of seconds the operation runs for each enhanced history bucket. For example, a value of 900 indicates that statistics were gathered for 15 minutes before the next bucket was created.
Bucket Index:	The number identifying the collection bucket. The number of buckets is set using the **enhanced-history** RTR configuration command.

show rtr enhanced-history distribution-statistics

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

To display enhanced history distribution statistics for Cisco IOS IP Service Level Agreements (IP SLAs) operations in tabular format, use the **show rtr enhanced-history distribution-statistics** command in user EXEC or privileged EXEC mode.

show rtr enhanced-history distribution-statistics [*operation-number* [**interval** *seconds*]]

Syntax Description

operation-number	(Optional) Displays enhanced history distribution statistics for only the specified operation.
interval *seconds*	(Optional) Displays enhanced history distribution statistics for only the specified aggregation interval for only the specified operation. • The range is from 1 to 3600 (1 hour). The default is 900.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(14)T	This command was replaced by the **show ip sla monitor enhanced-history distribution-statistics** 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 **show ip sla monitor enhanced-history distribution-statistics** command.
12.2(33)SRB	This command was replaced by the **show ip sla enhanced-history distribution-statistics** command.

Usage Guidelines

The distribution statistics consist of the following:

- The sum of completion times (used to calculate the mean)
- The sum of the completion times squared (used to calculate standard deviation)
- The maximum and minimum completion times

- The number of completed attempts

You can also use the following commands to display additional statistics or history information, or to view the status of the operation:

- **show rtr enhanced-history collection-statistics**
- **show rtr enhanced-history totals-statistics**

Tip If the character 'n' appears in your output, or not all fields are displayed, you should increase the screen width for your CLI display (for example, using the **width** line configuration command or the **terminal width** EXEC mode command).

Examples

The following is sample output from the **show rtr enhanced-history distribution-statistics** command. The fields are defined at the beginning of the output for the command. RTT means round-trip-time.

```
Router# show rtr enhanced-history distribution-statistics 3

 Point by point Enhanced History

Entry    = Entry Number
Int      = Aggregation Interval (seconds)
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT    Pth Hop Comps OvrTh SumCmp   SumCmp2L  SumCmp2H   TMax     TMin
3     900 1    257850000 1   1   3     0     43       617        0          15       14
3     900 2    258750002 1   1   3     0     45       677        0          16       14
3     900 3    259650000 1   1   3     0     44       646        0          15       14
3     900 4    260550002 1   1   3     0     42       594        0          15       12
3     900 5    261450003 1   1   3     0     42       590        0          15       13
3     900 6    262350001 1   1   3     0     46       706        0          16       15
3     900 7    263250003 1   1   3     0     46       708        0          16       14
 .
 .
 .
```

The time elapsed between BucketIndex 1 (started at 257,850,000) and BucketIndex 2 (started at 258,750,002) in this example is 900,002 milliseconds, or 900 seconds.

Table 67 describes the significant fields shown in the display.

Table 67 show rtr enhanced-history distribution-statistics Field Descriptions

Field	Description
Entry	The operation ID number you specified for the IP SLAs operation.
Int	Aggregation interval—The configured statistical distribution buckets interval, in seconds. For example, a value of 900 for Int means that statistics are gathered for 900 seconds per bucket.
BucI	Bucket index number—A number uniquely identifying the statistical distribution (aggregation) bucket. The number of history buckets to be kept is configured using the **buckets-of-history-kept** command. A bucket will gather statistics for the specified interval of time (aggregation interval), after which a new statistics bucket is created. If a number-of-buckets-kept value is configured, the interval for the last bucket is infinity (until the end of the operation). Buckets are not applicable to HTTP and UDP jitter monitoring operations. This field is equivalant to the rttMonStatsCaptureDistIndex object in the Cisco RTTMON MIB.
StartT	Aggregation start time—Start time for the aggregation interval (per Bucket Index). Shows the start time as the number of milliseconds since the router started; in other words, the time stamp is the number of milliseconds since the last system bootup.
Pth	Path index number—An identifier for a set of different paths to the target destination that have been discovered. For example, if the first operation iteration finds the path h1, h2, h3, h4, then this path is labeled as 1. If, on a later iteration, a new path is discovered, (such as h1, h2, h5, h6, h4) then this new path will be identified as 2, and so on. Data collection per path is available only for ICMP path echo operations (“pathEcho probes”). For all other operations, a value of 1 will always appear. Data collection per path is configured using the **paths-of-statistics-kept** *number* command when configuring the operation.

Table 67 show rtr enhanced-history distribution-statistics Field Descriptions (continued)

Field	Description
Hop	Hop Index Number—Statistics data per hop. A hop is data transmission between two points in a path (for example, from device h2 to device h3). Data collection per hop is available only for ICMP path echo operations ("pathEcho probes"). For all other operations, a value of "1" will always appear. Data collection per hop is configured using the **hops-of-statistics-kept** *number* command when configuring the operation. This field is equivalent to the rrttMonStatsCaptureHopIndex object in the Cisco RTTMON MIB.
Comps	Completions—The number of round-trip time operations that have completed without an error and without timing out, per bucket index. This object has the special behavior as defined by the ROLLOVER NOTE in the DESCRIPTION of the Cisco Rttmon MIB object.
SumCmp	Sum of completed operation times (1)—The total of all round-trip time values for all succesful operations in the row, in milliseconds.

Table 67 show rtr enhanced-history distribution-statistics Field Descriptions (continued)

Field	Description
SumCmp2L	Sum of the squares of completed operation times (2), Low-Order—The sum of the square roots of round-trip times for operations that were successfully measured, in milliseconds; displays the low-order 32 bits of the value only. • 32 low-order bits and 32 high-order bits are ordered in unsigned 64-bit integers (Int64) as follows: --- | High-order 32 bits | Low-order 32 bits | --- • The "SumCmp2" values are split into "high-order" and "low-order" numbers because of limitations of Simple Network Management Protocol (SNMP). The maximum value allowed for an SNMP object is 4,294,967,295 (the Gauge32 limit). If the sum of the square roots for your operation exceeds this value, then the "high-order" value will be utilized. (For example, the number 4,294,967,296 would have all low-order bits as 0, and the right-most high-order bit would be 1). • The low-order value (SumCmp2L) appears first in the output because in most cases, the value will be less than 4,294,967,295, which means that the value of SumCmp2H will appear as zero.
SumCmp2H	Sum of the squares of completed operation times (2), High-Order—The high-order 32 bits of the accumulated squares of completion times (in milliseconds) of operations that completed successfully.
TMax	Round-trip time, maximum—The highest recorded round-trip time, in milliseconds, per aggregation interval.
TMin	Round-trip time, minimum—The lowest recorded round-trip time, in milliseconds, per aggregation interval.

Related Commands

Command	Description
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
show rtr enhanced-history collection-statistics	Displays data for all collected history buckets for the specified IP SLAs operation, with data for each bucket shown individually.

show rtr group schedule

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

To display the group schedule details of Cisco IOS IP Service Level Agreements (IP SLAs) operations, use the **show rtr group schedule** command in user EXEC or privileged EXEC mode.

show rtr group schedule [*group-operation-number*]

Syntax Description

group-operation-number	(Optional) Number of the IP SLAs group operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **show 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 **show ip sla monitor group schedule** command.
12.2(33)SRB	This command was replaced by the **show ip sla group schedule** command.

Examples

The following is sample output from the **show rtr group schedule** command that shows information about group (multiple) scheduling. The last line in the example indicates that the IP SLAs operations are multiple scheduled (TRUE):

```
Router# show rtr group schedule

Multi-Scheduling Configuration:
Group Entry Number: 1
Probes to be scheduled: 2,3,4,9-30,89
Schedule period :60
Group operation frequency: 30
Multi-scheduled: TRUE
```

The following is sample output from the **show rtr group schedule** command that shows information about group (multiple) scheduling, with the **frequency** value the same as the **schedule-period** value, the **life** value as 3600 seconds, and the **ageout** value as never:

```
Router# show rtr group schedule
Group Entry Number: 1
Probes to be scheduled: 3,4,6-10
Total number of probes: 7
Schedule period: 20
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Start Time already passed
Life (seconds): 3600
Entry Ageout (seconds): never
```

Table 68 describes the significant fields shown in the displays.

Table 68 show rtr group schedule Field Descriptions

Field	Description
Group Entry Number	The operation group number specified for IP SLAs multiple operations scheduling.
Probes to be scheduled	The operations numbers specified in the operation group 1.
Scheduled period	The time in seconds you mentioned while scheduling the operation.
Group operation frequency	The frequency at which each operation is started.
Multi-scheduled	The value TRUE shows that group scheduling is active.

Related Commands

Command	Description
show rtr configuration	Displays the scheduling details.
show running configuration	Displays the configuration details which includes the IP SLAs multiple operations scheduling information.

show rtr history

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

To display history collected for all Cisco IOS IP Service Level Agreements (IP SLAs) operations or for a specified operation, use the **show rtr history** command in user EXEC or privileged EXEC mode.

show rtr history [*operation-number*] [**tabular** | **full**]

Syntax Description

operation-number	(Optional) Displays history for only the specified operation.
tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information. This is the default.
full	(Optional) Displays all information using identifiers next to each displayed value.

Defaults

Tabular format history for all operations is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Table 69 lists the Response Return values used in the output of the **show rtr history** command. If the default (**tabular**) format is used, the Response Return description is displayed as a code in the Sense column. If the full format is used, the Response Return is displayed as indicated in the Description column.

Table 69 Response Return (Sense Column) Codes

Code	Description
1	Okay.
2	Disconnected.
3	Over threshold.

Table 69 Response Return (Sense Column) Codes (continued)

Code	Description
4	Timeout.
5	Busy.
6	Not connected.
7	Dropped.
8	Sequence error.
9	Verify error.
10	Application specific.

Examples

The following is sample output from the **show rtr history** command in tabular format:

```
Router# show rtr history

        Point by point History
          Multiple Lines per Entry
Line 1
 Entry    = Entry Number
 LifeI    = Life Index
 BucketI  = Bucket Index
 SampleI  = Sample Index
 SampleT  = Sample Start Time
 CompT    = Completion Time (milliseconds)
 Sense    = Response Return Code
Line 2 has the Target Address
Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense
2     1          1          1          17436548   16          1
  AB 45 A0 16
2     1          2          1          17436551   4           1
  AC 12 7  29
2     1          2          2          17436551   1           1
  AC 12 5  22
2     1          2          3          17436552   4           1
  AB 45 A7 22
2     1          2          4          17436552   4           1
  AB 45 A0 16
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show rtr mpls-lsp-monitor configuration

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

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

show rtr mpls-lsp-monitor configuration [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the LSP Health Monitor operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(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 **show ip sla monitor mpls-lsp-monitor configuration** command.
12.2(33)SRB	This command was replaced by the **show ip sla mpls-lsp-monitor configuration** command.

Usage Guidelines

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

Examples

The following is sample output from the **show rtr mpls-lsp-monitor configuration** command:

```
Router# show rtr mpls-lsp-monitor configuration 1

Entry Number : 1
Modification time   : *12:18:21.830 PDT Fri Aug 19 2005
Operation Type      : echo
Vrf Name            : saa-vrf-all
Tag                 :
EXP Value           : 0
Timeout(ms)         : 1000
Threshold(ms)       : 5000
```

```
Frequency(sec)      : Equals schedule period
LSP Selector        : 127.0.0.1
ScanInterval(min)   : 1
Delete Scan Factor  : 1
Operations List     : 100001-100003
Schedule Period(sec): 60
Request size        : 100
Start Time          : Start Time already passed
SNMP RowStatus      : Active
TTL value           : 255
Reply Mode          : ipv4
Reply Dscp Bits     :
Secondary Frequency : Enabled on Timeout
         Value(sec) : 10
Reaction Configs    :
    Reaction        : connectionLoss
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
    Reaction        : timeout
    Threshold Type  : Consecutive
    Threshold Count : 3
    Action Type     : Trap Only
```

Table 70 describes the significant fields shown in the display.

Table 70 show rtr mpls-lsp-monitor configuration Field Descriptions

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

Table 70 show rtr mpls-lsp-monitor configuration Field Descriptions (continued)

Field	Description
Delete Scan Factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
Operations List	Identification numbers IP SLAs operations created by the LSP Health Monitor operation.
Schedule Period(sec)	Amount of time for which the LSP Health Monitor operation is scheduled.
Request size	Protocol data size for the request packet of the IP SLAs operation.
Start Time	Status of the start time for the LSP Health Monitor operation.
SNMP RowStatus	Indicates whether SNMP RowStatus is active or inactive.
TTL value	The maximum hop count for an echo request packet of the IP SLAs operation.
Reply Mode	Reply mode for an echo request packet of the IP SLAs operation.
Reply Dscp Bits	Differentiated services codepoint (DSCP) value of an echo reply packet of the IP SLAs operation.
Secondary Frequency	Reaction condition that will enable the secondary frequency option.
Value(sec)	Secondary frequency value.
Reaction Configs	Reaction configuration of the IP SLAs operation.
Reaction	Reaction condition being monitored.
Threshold Type	Specifies when an action should be performed as a result of a reaction event.
Threshold Count	The number of times a reaction event can occur before an action should be performed.
Action Type	Type of action that should be performed as a result of a reaction event.

Related Commands

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

show rtr mpls-lsp-monitor neighbors

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

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

show rtr mpls-lsp-monitor neighbors

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

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

```
Router# show rtr mpls-lsp-monitor neighbors

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

Table 71 describes the significant fields shown in the display.

Table 71 show rtr mpls-lsp-monitor neighbors Field Descriptions

Field	Description
BGP Next hop	Identifier for the BGP next hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
ProbeID	The identification number of the IP SLAs operation. The names of the VRFs that contain routing entries for the specified BGP next hop neighbor are listed in parentheses.
OK	LSP ping or LSP traceroute connectivity status between the source PE router and specified BGP next hop neighbor. Connectivity status can be the following: • OK—Successful reply. • ConnectionLoss—Reply is from a device that is not egress for the Forward Equivalence Class (FEC). • Timeout—Echo request timeout. • Unknown—State of LSP is not known.

Related Commands

Command	Description
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 scan-queue

Note Effective with Cisco IOS Release 12.2(31)SB2, the **show rtr mpls-lsp-monitor scan-queue** command is replaced by the **show ip sla monitor mpls-lsp-monitor scan-queue** command. Effective with Cisco IOS Release 12.2(33)SRB, the **show rtr mpls-lsp-monitor scan-queue** command is replaced by the **show ip sla mpls-lsp-monitor scan-queue** command. See the **show ip sla monitor mpls-lsp-monitor scan-queue** and **show ip sla mpls-lsp-monitor scan-queue** commands for more information.

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

show rtr mpls-lsp-monitor scan-queue *operation-number*

Syntax Description

operation-number	Number of the LSP Health Monitor operation for which the details will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(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 **show ip sla monitor mpls-lsp-monitor scan-queue** command.
12.2(33)SRB	This command was replaced by the **show ip sla mpls-lsp-monitor scan-queue** command.

Examples

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

```
Router# show rtr mpls-lsp-monitor scan-queue 1

Next scan Time after: 23 Secs
Next Delete scan Time after: 83 Secs

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

Table 72 describes the significant fields shown in the display.

Table 72 show rtr mpls-lsp-monitor scan-queue Field Descriptions

Field	Description
Next scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about adding BGP next hop neighbors to a particular VPN. At the start of each scan time, IP SLAs operations are created for all newly discovered neighbors.
Next Delete scan Time after	Amount of time left before the LSP Health Monitor checks the scan queue for information about deleting BGP next hop neighbors from a particular VPN. At the start of each delete scan time, IP SLAs operations are deleted for neighbors that are no longer valid.
BGP Next hop	Identifier for the BGP next hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next hop neighbor to be used by the MPLS LSP ping operation.
vrf	Name of the VRF that contains a routing entry for the specified BGP next hop neighbor.
Add/Delete	Indicates that the specified BGP next hop neighbor will be added to or removed from the specified VPN.

Related Commands

Command	Description
delete-scan-factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
mpls discovery vpn interval	Specifies the time interval at which routing entries that are no longer valid are removed from the BGP next hop neighbor discovery database of an MPLS VPN.
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.
scan-interval	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.

show rtr operational-state

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

To display the operational state of all Cisco IOS IP Service Level Agreements (IP SLAs) operations or a specified operation, use the **show rtr operational-state** command in user EXEC or privileged EXEC mode.

show rtr operational-state [*operation-number*]

Syntax Description

operation-number	(Optional) ID number of the IP SLAs operation to display.

Defaults

Displays output for all running IP SLAs operations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	Output for the Jitter operation type was added.
12.1	The **tabular** and **full** keywords were removed.
12.2(8)T	Output for “NumOfJitterSamples” was added (CSCdv30022).
12.2(8)S	Output for “NumOfJitterSamples” was added (CSCdv30022).
12.3(4)T	Output (MOS and ICPIF scores) for the Jitter (codec) operation type was added.
12.3(7)T	Decimal granularity for MOS scores was added.
12.3(14)T	This command was replaced by the **show ip sla monitor statistics** command.
12.2(31)SB2	This command was replaced by the **show ip sla monitor statistics** command.
12.2(33)SRB	This command was replaced by the **show ip sla statistics** command.

Usage Guidelines

Use the **show rtr operational-state** command to display the current state of IP SLAs operations, including how much life the operation has left, whether the operation is active, and the completion time. The output will also include the monitoring data returned for the last (most recently completed) operation.

Examples

The following example shows basic sample output from the **show rtr operational-state** command:

```
Router# show rtr operational-state
        Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

The following example shows sample output from the **show rtr operational-state** command when the specified operation is a Jitter (codec) operation:

```
Router# show rtr operational-state 1
Entry number: 1
Modification time: 13:18:38.012 PST Mon Jun 24 2002
Number of Octets Used by this Entry: 10392
Number of operations attempted: 2
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 2
Latest operation start time: *13:18:42.896 PST Mon Jun 24 2002
Latest operation return code: OK
Voice Scores:
ICPIF Value: 0  MOS score: 0
RTT Values:
NumOfRTT: 61    RTTAvg: 2       RTTMin: 2       RTTMax: 3
RTTSum: 123     RTTSum2: 249
Packet Loss Values:
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0       PacketSkipped: 39   <<<<<<==========
Jitter Values:
MinOfPositivesSD: 1     MaxOfPositivesSD: 1
NumOfPositivesSD: 1     SumOfPositivesSD: 1     Sum2PositivesSD: 1
MinOfNegativesSD: 1     MaxOfNegativesSD: 1
NumOfNegativesSD: 1     SumOfNegativesSD: 1     Sum2NegativesSD: 1
MinOfPositivesDS: 0     MaxOfPositivesDS: 0
NumOfPositivesDS: 0     SumOfPositivesDS: 0     Sum2PositivesDS: 0
MinOfNegativesDS: 0     MaxOfNegativesDS: 0
NumOfNegativesDS: 0     SumOfNegativesDS: 0     Sum2NegativesDS: 0
Interarrival jitterout: 0       Interarrival jitterin: 0
One Way Values:
NumOfOW: 0
OWMinSD: 0      OWMaxSD: 0      OWSumSD: 0      OWSum2SD: 0
OWMinDS: 0      OWMaxDS: 0      OWSumDS: 0      OWSum2DS: 0
```

The values shown indicate the values for the last IP SLAs operation. RTT stands for Round-Trip-Time. SD stands for Source-to-Destination. DS stands for Destination-to-Source. OW stands for One Way. The * symbol in front of the time stamps indicates the time is synchronized using NTP or SNTP. Table 73 describes the significant fields shown in this output.

Table 73 show rtr operational-state Field Descriptions

Field	Description
Voice Scores:	Indicates that Voice over IP statistics appear on the following lines. Voice score data is computed when the operation type is configured as **type jitter (codec)**.
ICPIF:	The Calculated Planning Impairment Factor (ICPIF) value for the latest iteration of the operation. The ICPIF value is computed by IP SLAs using the formula *Icpif = Io + Iq + Idte + Idd + Ie – A*, where • the values for *Io*, *Iq*, and *Idte* are set to zero, • the value *Idd* is computed based on the measured one way delay, • the value *Ie* is computed based on the measured packet loss, • and the value of A is specified by the user. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically less than 20 are generally considered “adequate.” **Note** This value is intended only for relative comparisons, and may not match ICPIF values generated using alternate methods.
MOS:	The estimated Mean Opinion Score (Conversational Quality, Estimated) for the latest iteration of the operation. The MOS-CQE is computed by IP SLAs as a function of the ICPIF. MOS values are expressed as a number from 1 (1.00) to 5 (5.00), with 5 being the highest level of quality, and 1 being the lowest level of quality. A MOS value of 0 (zero) indicates that MOS data could not be generated for the operation.
RTT Values:	Indicates that Round-Trip-Time statistics appear on the following lines.
NumOfRTT	The number of successful round trips.
RTTSum	The sum of those round trip values (in milliseconds).
RTTSum2	The sum of squares of those round trip values (in milliseconds).
Packet Loss Values:	Indicates that Packet Loss statistics appear on the following lines.
PacketLossSD	The number of packets lost from source to destination.
PacketLossDS	The number of packets lost from destination to source.
PacketOutOfSequence	The number of packets returned out of order.
PacketMIA	The number of packets lost where the direction (SD or DS) cannot be determined (MIA: “missing in action”).

Table 73 show rtr operational-state Field Descriptions (continued)

Field	Description
PacketLateArrival	The number of packets that arrived after the timeout.
PacketSkipped	The number of packets that are not sent during the IP SLAs jitter operation.
InternalError	The number of times an operation could not be started due to other internal failures.
Busies	The number of times this operation could not be started because the previously scheduled run was not finished.
Jitter Values:	Indicates that jitter operation statistics appear on the following lines. Jitter is inter-packet delay variance.
NumOfJitterSamples:	The number of jitter samples collected. This is the number of samples that are used to calculate the following jitter statistics.
MinOfPositivesSD MaxOfPositivesSD	The minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	The number of jitter values from source to destination that are positive (i.e., network latency increases for two consecutive test packets).
SumOfPositivesSD	The sum of those positive values (in milliseconds).
Sum2PositivesSD	The sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	The minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	The number of jitter values from source to destination that are negative (that is, network latency decreases for two consecutive test packets).
SumOfNegativesSD	The sum of those values.
Sum2NegativesSD	The sum of the squares of those values.
Interarrival jitterout:	The source to destination (SD) jitter value calculation, as defined in RFC 1889.
Interarrival jitterin:	The destination to source (DS) jitter value calculation, as defined in RFC 1889.
One Way Values	Indicates that One Way measurement statistics appear on the following lines. One Way (OW) Values are the amount of time it took the packet to travel from the source router to the target router (SD) or from the target router to the source router (DS).
NumOfOW	Number of successful one way time measurements.
OWMinSD	Minimum time from the source to the destination.

Table 73 show rtr operational-state Field Descriptions (continued)

Field	Description
OWMaxSD	Maximum time from the source to the destination.
OWSumSD	Sum of the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show rtr reaction-configuration

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

To display the configured proactive threshold monitoring settings for all Cisco IOS IP Service Level Agreements (SLAs) operations or a specified operation, use the **show rtr reaction-configuration** command in user EXEC or privileged EXEC mode.

show rtr reaction-configuration [*operation-number*]

Syntax Description

operation-number	(Optional) Displays the reaction configuration for only the specified IP SLAs operation.

Defaults

Displays configured proactive threshold monitoring settings for all IP SLAs operations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(14)T	This command was replaced by the **show ip sla monitor reaction-configuration** 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 **show ip sla monitor reaction-configuration** command.
12.2(33)SRB	This command was replaced by the **show ip sla reaction-configuration** command.

Usage Guidelines

Use the **rtr reaction-configuration** command in global configuration mode to configure the proactive threshold monitoring parameters for an IP SLAs operations.

Examples

In the following example, multiple monitored elements (indicated by the Reaction values) are configured for a single IP SLAs operation:

```
Router# show rtr reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None

Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly

Reaction: jitterDSAvg
Threshold type:  immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly

Reaction: PacketLossSD
Threshold type:  immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

Table 74 describes the significant fields shown in this output.

Table 74 show rtr reaction-configuration Field Descriptions

Field	Description
Reaction:	The monitored element configured for the specified IP SLAs operation. Corresponds to the **react** {**connectionLoss** | **jitterAvg** | **jitterDSAvg** | **jitterSDAvg** | **mos** | **PacketLossDS** | **PacketLossSD** | **rtt** | **timeout** | **verifyError**} syntax in the **rtr reaction-configuration** command.
Threshold type:	The configured threshold type. Corresponds to the **threshold-type** {**never** | **immediate** | **consecutive** | **xofy** | **average**} syntax in the **rtr reaction-configuration** command.
Rising (milliseconds):	The *upper-threshold* value, as configured by the **threshold-value** *upper-threshold lower-threshold* syntax in the **rtr reaction-configuration** command.

Table 74 show rtr reaction-configuration Field Descriptions (continued)

Field	Description
Threshold Falling (milliseconds):	The *lower-threshold* value, as configured by the **threshold-value** *upper-threshold lower-threshold* syntax in the **rtr reaction-configuration** command.
Threshold Count:	The *x-value* in the **xofy** threshold type, or the *number-of-measurements* value for **average** threshold type.
Threshold Count2:	The *y-value* in the **xofy** threshold-type.
Action Type:	The reaction to be performed when the violation conditions are met, as configured by the **action-type** {**none** | **trapOnly** | **triggerOnly** | **trapAndTrigger**} syntax in the **rtr reaction-configuration** command.

Related Commands

Command	Description
rtr reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.

show rtr reaction-trigger

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

To display the reaction trigger information for all Cisco IOS IP Service Level Agreements (IP SLAs) operations or the specified operation, use the **show rtr reaction-trigger** command in user EXEC or privileged EXEC mode.

show rtr reaction-trigger [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLAs operation to display.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Use the **show rtr reaction-trigger** command to display the configuration status and operational state of target operations that will be triggered as defined with the **rtr reaction-configuration** global command.

Examples

The following is sample output from the **show rtr reaction-trigger** command:

```
Router# show rtr reaction-trigger 1

        Reaction Table
Entry Number: 1
Target Entry Number: 2
Status of Entry (SNMP RowStatus): active
Operational State: pending
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

show rtr responder

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

To display Cisco IOS IP Service Level Agreements (IP SLAs) Responder information, use the **show rtr responder** command in user EXEC or privileged EXEC mode.

show rtr responder

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

Use the **show rtr responder** command to display information about recent sources of IP SLAs control messages, such as who has sent recent control messages and who has sent invalid control messages.

Examples

The following is sample output from the **show rtr responder** command:

```
Router# show rtr responder

RTR Responder is: Enabled
Number of control message received: 19 Number of errors: 1
Recent sources:
            4.0.0.1 [19:11:49.035 UTC Sat Dec 2 1995]
            4.0.0.1 [19:10:49.023 UTC Sat Dec 2 1995]
            4.0.0.1 [19:09:48.707 UTC Sat Dec 2 1995]
            4.0.0.1 [19:08:48.687 UTC Sat Dec 2 1995]
            4.0.0.1 [19:07:48.671 UTC Sat Dec 2 1995]

Recent error sources:
            4.0.0.1 [19:10:49.023 UTC Sat Dec 2 1995] RTT_AUTH_FAIL
```

Related Commands

Command	Description
show rtr configuration	Displays configuration values for IP SLAs operations.

show rtr totals-statistics

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

To display the total statistical values (accumulation of error counts and completions) for all Cisco IOS IP Service Level Agreements (IP SLAs) operations or the specified operation, use the **show rtr totals-statistics** command in user EXEC or privileged EXEC mode.

show rtr totals-statistics [*number*] [**tabular** | **full**]

Syntax Description

number	(Optional) Number of the IP SLAs operation to display.
tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

Defaults

Full format for all operations

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the **show ip sla monitor total-statistics** command.
12.2(31)SB2	This command was replaced by the **show ip sla monitor statistics aggregated** command.
12.2(33)SRB	This command was replaced by the **show ip sla statistics aggregated** command.

Usage Guidelines

The total statistics consist of the following items:

- The operation number
- The start time of the current hour of statistics
- The age of the current hour of statistics

- The number of attempted operations

You can also use the **show rtr distributions-statistics** and **show rtr collection-statistics** commands to display additional statistical information.

Examples

The following is sample output from the **show rtr totals-statistics** command in full format:

```
Router# show rtr totals-statistics

        Statistic Totals
Entry Number: 1
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Age of Statistics Entry (hundredths of seconds): 48252
Number of Initiations: 10
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all IP SLAs operations or the specified operation.
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all IP SLAs operations or the specified operation.

source-ip (tplt)

To specify an source IP address in an auto IP Service Level Agreements (SLAs) operation template, use the **source-ip** command in the appropriate submode of IP SLA template configuration mode. To remove the specified address from the configuration, use the **no** form of the command.

source-ip {*ip-address* | *hostname*}

no source-ip {*ip-address* | *hostname*}

Syntax Description

ip-address | *hostname*	IPv4 address or hostname of source.

Defaults

The source address for the operation template is the IP address closest to the destination.

Command Modes

IP SLA Template Configuration

ICMP echo configuration (config-tplt-icmp-ech
ICMP jitter configuration (config-tplt-icmp-jtr)
TCP connect configuration (config-tplt-tcp-conn)
UDP echo configuration (config-tplt-udp-ech)
UDP jitter configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command adds the specified source address to the configuration of an auto IP SLAs operation template. When a source IP address or hostname is not specified, auto IP SLAs chooses the IP address nearest to the destination.

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.

Examples

The following example shows how to configure the IP address and port number of the source in an auto IP SLAs operation template:

```
Router(config)#ip sla auto template type ip udp-jitter 1
Router(config-tplt-udp-jtr)# source-ip 10.1.1.1
Router(config-tplt-udp-jtr)# source-port 23
Router(config-tplt-udp-jtr# end
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: 1
    Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 10.1.1.1 Source Port: 23
        VRF:    TOS: 0x0
```

```
Operation Parameters:
    Request Data Size: 16   Verify Data: false
    Timeout: 5000           Threshold: 5000
Statistics Aggregation option:
    Hours of statistics kept: 2
History options:
    History filter: none
    Max number of history records kept: 15
    Lives of history kept: 0
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

Related Commands

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

source-port

To specify a source-port number in an auto Service Level Agreements (SLAs) operation template, use the **source-port** command in the appropriate submode of IP SLA template configuration mode. To remove the specified port from the configuration, use the **no** form of the command.

source-port *port-number*

no source-port *port-number*

Syntax Description

port-number	Port number of source.

Command Default

Auto IP SLAs chooses an available port.

Command Modes

IP SLA Template Configuration

TCP connect configuration (config-tplt-tcp-conn)
UDP echo configuration (config-tplt-udp-ech)
UDP jitter configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command adds the specified source-port number to the configuration of an auto IP SLAs operation template. When a source-port number is not specified, auto IP SLAs chooses an available port.

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.

Examples

The following example shows how to configure the IP address and port number of the source in an auto IP SLAs operation template:

```
Router(config)#ip sla auto template type ip udp-jitter 1
Router(config-tplt-udp-jtr)# source-ip 10.1.1.1
Router(config-tplt-udp-jtr)# source-port 23
Router(config-tplt-udp-jtr# end
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: 1
    Measure Type: udp-jitter (control enabled)
    Description:
    IP options:
        Source IP: 10.1.1.1 Source Port: 23
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 16   Verify Data: false
        Timeout: 5000           Threshold: 5000
```

```
Statistics Aggregation option:
    Hours of statistics kept: 2
History options:
    History filter: none
    Max number of history records kept: 15
    Lives of history kept: 0
Statistics Distributions options:
    Distributions characteristics: RTT
    Distributions bucket size: 20
    Max number of distributions buckets: 1
Reaction Configuration: None
```

Related Commands

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

start-time

To specify the start time in an auto IP Service Level Agreement (SLAs) scheduler, use the **start-time** command in IP SLAs auto-measure schedule configuration mode.

start-time {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}

Syntax Description

hh:*mm*[:*ss*]	Absolute start time, in 24-hour clock format with hours (*hh*), minutes (*mm*), and seconds (*ss*) separated by a colon (**:**). Seconds (:ss) are optional. Range is from 00:00:00 to 23:59:59, with 00:00 being midnight and 23:59 being 11:59 p.m. The colons (:) are required. Current month and day is default.
month day	(Optional) Start day other than today, in month then day format. Value for month is either the full English name or the first three letters of the month. Range for day is from 1 to 31.
day month	(Optional) Start day other than today, in day then month format. Range for day is from 1 to 31. Value for the month is either the full English name or the first three letters of the month.
pending	Spcifies that no information is collected. This is the default.
now	Spcifies that this operation starts immediately after this command is configured.
after *hh*:*mm*:*ss*	Specifies that start time is up to one 24-hour day after this command is configured, with hours (*hh*), minutes (*mm*), and seconds (*ss*) separated by a colon (**:**). Range is from 00:00:00 to 23:59:59. The colons (:) are required.

Command Default

The auto IP SLAs scheduler is enabled and the state of the scheduler is pending.

Command Modes

IP SLAs auto-measure schedule configuration (config-am-schedule)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the value of the start-time characteristic in the IP SLAs schedule from the default (pending) to the specified value.

If the operation being controlled by an auto IP SLAs scheduler is in a pending trigger (default) state, you can define the conditions under which the operation makes the transition from pending to active with the **react** command.

After you configure this command to specify a start time other than the default (pending), you cannot modify the auto IP SLAs scheduler. If you attempt to modify a scheduler with a specified start-time, the following message appears:

```
%Entry already scheduled and cannot be modified
```

To change the configuration of an auto IP SLAs scheduler in which the start time is other than the default, use the **no** form of the **ip slan auto schedule** command to remove the scheduler configuration and reenter the configuration information.

Examples

The following example shows how to configure an auto IP SLAs scheduler that will cause an auto IP SLAs operation to actively collect data at 3:00 p.m. on April 5. The operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished its life. When the operation ages out, all configuration information for the operation is removed from the running configuration in RAM:

```
Router(config)#ip sla auto schedule apr5
Router(config-am-schedule)#ageout 43200
Router(config-am-schedule)#frequency 70
Router(config-am-schedule)#life 43200
Router(config-am-schedule)#probe-interval 1500
Router(config-am-schedule)#start-time 15:00 apr 5
Router(config-am-schedule)#end
Router#
Router# show ip sla auto schedule apr5
Group sched-id: apr5
    Probe Interval (ms) : 1500
    Group operation frequency (sec): 70
    Status of entry (SNMP RowStatus): Active
    Next Scheduled Start Time: P15:00 apr 5
    Life (sec): 43200
    Entry Ageout (sec): 43200
Router#
```

Related Commands

Command	Description
ip sla auto schedule	Begins configuration for an auto IP SLAs scheduler and enters IP SLA auto-measure schedule configuration mode.
schedule	Specifies an auto IP SLAs scheduler for an IP SLAs auto-measure group.
react	Configures certain actions to occur based on events under the control of auto IP SLAs.
show ip sla auto schedule	Displays the configuration including default values of auto IP SLAs schedulers.

statistics-distribution-interval

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **statistics-distribution-interval** command is replaced by the **history statistics-distribution-interval** command. See the **history statistics-distribution-interval** command for more information.

To set the time interval for each statistics distribution kept for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **statistics-distribution-interval** command in the appropriate submode of IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

statistics-distribution-interval *milliseconds*

no statistics-distribution-interval

Syntax Description

milliseconds	Number of milliseconds (ms) used for each statistics distribution kept. The default is 20.

Defaults

20 ms

Command Modes

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **history statistics-distribution-interval** command.
12.2(33)SRB	This command was replaced by the **history statistics-distribution-interval** command.
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.

Release	Modification
12.2(33)SB	This command was replaced by the **history statistics-distribution-interval** command.
12.2(33)SXI	This command was replaced by the **history statistics-distribution-interval** command.

Usage Guidelines

In most situations, you do not need to change the time interval for each statistics distribution or number of distributions kept. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network. To set the number of statistics distributions kept, use the **distributions-of-statistics-kept** command.

Note 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.

Examples

In the following example, the statistics distribution is set to five and the distribution interval is set to 10 ms for IP SLAs ICMP echo operation 1. Consequently, the first distribution will contain statistics from 0 to 9 ms, the second distribution will contain statistics from 10 to 19 ms, the third distribution will contain statistics from 20 to 29 ms, the fourth distribution will contain statistics from 30 to 39 ms, and the fifth distribution will contain statistics from 40 ms to infinity.

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.161.21
 distributions-of-statistics-kept 5
 statistics-distribution-interval 10
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
distributions-of-statistics-kept	Sets the number of statistics distributions kept per hop during the IP SLAs operation's lifetime.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for the IP SLAs operation.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for the IP SLAs operation.

tag (IP SLA)

To create a user-specified identifier for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **tag** (IP SLA) command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, or IP SLA monitor configuration mode. To remove a tag from an operation, use the **no** form of this command.

tag *text*

no tag

Syntax Description

text	Name of a group to which the operation belongs. In Cisco IOS Release 12.2(33)SXF and earlier releases, the length of the tag is limited to 90 characters, including spaces.

Command Default

No tag identifier is specified.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

Auto IP SLA MPLS Configuration

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

IP SLA Auto Ethernet Configuration

Ethernet parameters configuration (config-ip-sla-ethernet-params)

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)

ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

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.
12.2(33)SRB	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
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 following configuration modes were added: • Ethernet echo • Ethernet jitter • Ethernet parameters • VCCV
12.4(20)T	This command was modified. The 90-character limit on the length of the *text* argument was removed and the Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
12.2(33)H	This command was modified. The 90-character limit on the length of the *text* argument was removed.
12.2(33)SXI	This command was modified. The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.

Usage Guidelines

An operation tag is normally used to logically link operations in a group.

Tags can be used to support automation (for example, by using the same tag for two different operations on two different routers echoing the same target).

In releases prior to Cisco IOS Release 12.2(33)SXH, the length of the *text* argument is limited to 90 characters, including spaces. If you configure a tag that is longer than 90 characters, including spaces, the device crashes because of a block overrun. In Cisco IOS Release 12.2(33)SXF and earlier releases, we recommend that you limit the length of the tag to approximately 80 characters, including spaces.

In Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(20)T, the 90-character limitation for the *text* argument was removed.

The **tag** (IP SLA) 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 75). Note that if you are configuring an IP SLAs label switched path (LSP) Health Monitor operation, see Table 76 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 **tag** (IP SLA) command varies depending on the Cisco IOS release you are running and the operation type configured.

Table 75 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 , 12.2(58)SE, 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 76 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

In the following examples, an IP SLAs ICMP echo operation is tagged with the label testoperation.

IP SLA Configuration

This example shows the **tag** (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA configuration mode:

```
ip sla 1
 icmp-echo 172.16.1.176
 tag testoperation
!
ip sla schedule 1 life forever start-time now
```

IP SLA Monitor Configuration

This example shows the **tag** (IP SLA) command being used in an IPv4 network in ICMP echo configuration mode within IP SLA monitor configuration mode:

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 tag testoperation
!
ip sla monitor schedule 1 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.

tcp-connect

To define a Cisco IOS IP Service Level Agreements (SLAs) Transmission Control Protocol (TCP) connection operation, use the **tcp-connect** command in IP SLA configuration mode.

tcp-connect {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname.
destination-port	Specifies the destination port number.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
control {**enable** | **disable**}	(Optional) Enables or disables the IP SLAs control protocol to send a control message to the IP SLAs Responder prior to sending an operation packet. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder.

Defaults

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type tcpConnect dest-ipaddr** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type tcpConnect dest-ipaddr** command.
12.2(33)SRC	Support for IPv6 addresses was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type tcpConnect dest-ipaddr** command. Support for IPv6 addresses was added.
12.4(20)T	Support for IPv6 addresses was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type tcpConnect dest-ipaddr** command.

Usage Guidelines

The TCP connection operation is used to discover the time required to connect to the target device. This operation can be used to test virtual circuit availability or application availability. If the target is a Cisco router, then IP SLAs makes a TCP connection to any port number specified by the user. If the destination is a non-Cisco IP host, then the user must specify a known target port number (for example, 21 for FTP, 23 for Telnet, or 80 for HTTP server). This operation is useful in testing Telnet or HTTP connection times.

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

You must enable the IP SLAs Responder on the target router before you can configure a TCP Connect operation.

Control protocol is required when the target device is a Cisco router that does not natively provide the UDP or TCP Connect service. Prior to sending an operation packet to the target router, IP SLAs sends a control message to the IP SLAs Responder to enable the destination port. If you disable control by using the **control disable** keyword combination with this command, you must define the IP address of the source for the Cisco IOS IP SLAs Responder by using the **ip sla responder tcp-connect ipaddress** command on the destination device.

IP SLAs TCP connect operations support both IPv4 and IPv6 addresses.

Examples

In the following example, IP SLAs operation 11 is configured as a TCP connection operation using the destination IP address 172.16.1.175 and the destination port 2400:

```
ip sla 11
 tcp-connect 172.16.1.175 2400
!
ip sla schedule 11 start-time now life forever
```

In the following example, IP SLAs operation 12 is configured as a TCP connection operation using the destination IPv6 address 2001:0DB8:200::FFFE and the destination port 2400:

```
ip sla 12
 tcp-connect 2001:0DB8:200::FFFE
!
ip sla schedule 12 start-time now life forever
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla responder tcp-connect ipaddress	Permanently enables IP SLAs Responder functionality on specified IP address and port.

template (am-group)

To add a auto IP Service Level Agreements (SLAs) operation template to the configuration of an IP SLAs auto-measure group, use the **template** command in IP SLA auto-measure group configuration mode. To remove the template from the configuration and restore the default, use the **no** form of this command.

template *operation*

no template

Syntax Description

operation	Type of IP operation. Use one of the following keywords: • **icmp-echo**—Internet Control Message Protocol (ICMP) echo operation • **icmp-jitter—**Internet Control Message Protocol (ICMP) jitter operation • **tcp-connect—**Transmission Control Protocol (TCP) connection operation • **udp-echo—**User Datagram Protocol (UDP) echo operation • **udp-jitter—**User Datagram Protocol (UDP) jitter operation

Command Default

Type of operation for the auto-measure group being configured is ICMP jitter.

Command Modes

IP SLA auto-measure group configuration (config-am-grp)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command changes the operation for the auto-measure group being configured from the default (ICMP jitter) to the operation defined in the specified template.

Only one auto IP SLAs operation template can be specified for each IP SLAs auto-measure group. Each operation template can be referenced by more than one group.

If no auto IP SLAs operation template is specified for an auto-measure group, the operation for the group is ICMP jitter (default).

If you issue this command and the specified template does not exist, the auto-measure group operations cannot start. If you configure the specified template after using this command, the template is added to the group configuration and scheduling can proceed.

To change the operation of an existing auto-measure group, first use the **no** form of this command to delete the auto IP SLAs operation template from the group configuration and then reconfigure the group with either a different or no operation template.

To configure an auto IP SLAs operation template, use the **ip sla auto template** command.

Examples

The following example shows how to add an auto IP SLAs endpoint list to the configuration of an IP SLAs auto-measure group:

```
Router(config)#ip sla auto group type ip 1
Router(config-am-grp)#template 1
Router(config-am-grp)#destination 1
Router(config-am-grp)#schedule 1
Router(config-am-grp)#end
Router#
Router#show ip sla auto group
Group Name: 1
    Description:
    Activation Trigger: Immediate
    Destination: 1
    Schedule: 1

IP SLAs Auto Template: 1
    Measure Type: icmp-jitter
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None

IP SLAs auto-generated operations of group 1
    no operation created
```

Related Commands

Command	Description
ip sla auto template	Enters IP SLA auto-measure template configuration mode and begins creating an auto IP SLAs operation template.

threshold (IP SLA)

To set the upper threshold value for calculating network monitoring statistics created by a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **threshold** command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, IP SLA auto Ethernet configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

threshold *milliseconds*

no threshold

Syntax Description

milliseconds	Length of time required for a rising threshold to be declared, in milliseconds (ms). Range is 0 to 60000. Default is 5000.

Command Default

The default is 5000 ms.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

Auto IP SLA MPLS Configuration

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

IP SLA auto Ethernet Configuration

Ethernet parameters configuration (config-ip-sla-ethernet-params)

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)

ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

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.
12.2(33)SRB	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
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 following configuration modes were added: • Ethernet echo • Ethernet jitter • Ethernet parameters • VCCV
12.4(20)T	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
12.2(33)SXI	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
15.1(1)T	This command was modified. The IP SLA template parameters configuration mode was added.

Usage Guidelines

The value specified for this command must not exceed the value specified for the **timeout** command.

The threshold value configured by this command is used only to calculate network monitoring statistics created by a Cisco IOS IP SLAs operation. This value is not used for generating Simple Network Management Protocol (SNMP) trap notifications. Use the **ip sla reaction-configuration** command in global configuration mode to configure the thresholds for generating IP SLAs SNMP trap notifications. For auto IP SLAs in Cisco IOS IP SLA Engine 3.0, use the **react** command to configure the thresholds for generating IP SLAs SNMP trap notifications.

For the IP SLAs User Datagram Protocol (UDP) jitter operation, the **threshold** (IP SLA) command sets the upper threshold value for the average jitter calculation. For all other IP SLAs operations, the **threshold** (IP SLA) command sets the upper threshold value for the round-trip time (RTT) measurement. IP SLAs will calculate the number of times the average jitter or RTT measurement exceeds the specified threshold value.

Consider the following guidelines before configuring the **frequency** (IP SLA), **timeout** (IP SLA), and **threshold** (IP SLA) commands. For the IP SLAs UDP jitter operation, the following guidelines are recommended:

- (**frequency** *seconds*) > ((**timeout** *milliseconds*) + N)
- (**timeout** *milliseconds*) > (**threshold** *milliseconds*)

where N = (**num-packets** *number-of-packets*) * (**interval** *interpacket-interval*). If you are running Cisco IOS IP SLAs Engine 3.0, use the **num-packets** command and the **interval** (params) commands to configure the values that define N. Otherwise, use the **udp-jitter** command to configure the **num-packets** *number-of-packets* and **interval** *interpacket-interval* values.

For all other IP SLAs operations, the following configuration guideline is recommended:

(**frequency** *seconds*) > (**timeout** *milliseconds*) > (**threshold** *milliseconds*)

The **threshold** (IP SLA) command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure 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 77). If you are configuring an IP SLAs label switched path (LSP) Health Monitor operation, see Table 78 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 **threshold** command varies depending on the Cisco IOS release you are running and the operation type configured.

If you are running Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **threshold** command.

Table 77 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Table 78 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 configure the threshold of the IP SLAs ICMP echo operation to 2500.

IP SLA Configuration

```
ip sla 1
 icmp-echo 172.16.1.176
 threshold 2500
!
ip sla schedule 1 start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 threshold 2500
!
ip sla monitor schedule 1 start-time now
```

IP SLA Template Parameters Configuration

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)# parameters
Router(config-icmp-ech-params)# timeout 2500
Router(config-icmp-ech-params)# threshold 2500
Router(config-icmp-ech-params)# end
Router#
00:02:26: %SYS-5-CONFIG_I: Configured from console by console
Router# show ip sla auto template type ip udp-echo
IP SLAs Auto Template: 1
    Measure Type: udp-echo (control enabled)
    Description:
.
.
.
    Operation Parameters:
        Request Data Size: 16   Verify Data: false
        Timeout: 2500 Threshold: 2500
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

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.
ip sla monitor reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.
ip sla reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.
react	Configures reaction and proactive threshold monitoring parameters in an auto IP SLAs operation template
timeout	Sets the amount of time the IP SLAs operation waits for a response from its request packet.

timeout (IP SLA)

To set the amount of time a Cisco IOS IP Service Level Agreements (SLAs) operation waits for a response from its request packet, use the **timeout** (IP SLA) command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, IP SLA auto Ethernet configuration, IP SLA monitor configuration or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

timeout *milliseconds*

no timeout

Syntax Description

milliseconds	Length of time the operation waits to receive a response from its request packet, in milliseconds (ms). Range is 0 to 604800000. We recommend that the value of the *milliseconds* argument be based on the sum of both the maximum round-trip time (RTT) value for the packets and the processing time of the IP SLAs operation.

Command Default

The default timeout value varies depending on the type of IP SLAs operation you are configuring.

Command Modes

IP SLA Configuration

DHCP configuration (config-ip-sla-dhcp)
DLSw configuration (config-ip-sla-dlsw)
DNS configuration (config-ip-sla-dns)
Ethernet echo (config-ip-sla-ethernet-echo)
Ethernet jitter (config-ip-sla-ethernet-jitter)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)
VCCV configuration (config-sla-vccv)
VoIP configuration (config-ip-sla-voip)

Auto IP SLA MPLS Configuration

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

IP SLA auto Ethernet Configuration

Ethernet parameters configuration (config-ip-sla-ethernet-params)

IP SLA Monitor Configuration

DHCP configuration (config-sla-monitor-dhcp)
DLSw configuration (config-sla-monitor-dlsw)
DNS configuration (config-sla-monitor-dns)
FTP configuration (config-sla-monitor-ftp)
HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)
VoIP configuration (config-sla-monitor-voip)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
ICMP jitter configuration (config-icmp-jtr-params)
TCP connect configuration (config-tcp-conn-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

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.
12.2(33)SRB	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
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 following configuration modes were added: • Ethernet echo • Ethernet jitter • Ethernet parameters • VCCV
12.4(20)T	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
12.2(33)SXI	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
15.1(1)T	This command was modified. The IP SLA template parameters configuration mode was added.

Usage Guidelines

We recommend that the value of the *milliseconds* argument be based on the sum of both the maximum round-trip time (RTT) value for the packets and the processing time of the IP SLAs operation.

Use the **timeout** (IP SLA) command to set how long the operation waits to receive a response from its request packet, and use the **frequency** (IP SLA) command to set the rate at which the IP SLAs operation restarts. The value specified for the **timeout** (IP SLA) command cannot be greater than the value specified for the **frequency** (IP SLA) command.

Consider the following guidelines before configuring the **frequency** (IP SLA), **timeout** (IP SLA), and **threshold** (IP SLA) commands. For the IP SLAs User Datagram Protocol (UDP) jitter operation, the following guidelines are recommended:

- (**frequency** *seconds*) > ((**timeout** *milliseconds*) + N)
- (**timeout** *milliseconds*) > (**threshold** *milliseconds*)

where N = (**num-packets** *number-of-packets*) * (**interval** *interpacket-interval*). If you are running Cisco IOS IP SLAs Engine 3.0, use the **num-packets** command and the **interval** (params) commands to configure the values that define N. Otherwise, use the **udp-jitter** command to configure the **num-packets** *number-of-packets* and **interval** *interpacket-interval* values.

For all other IP SLAs operations, the following configuration guideline is recommended:

(**frequency** *seconds*) > (**timeout** *milliseconds*) > (**threshold** *milliseconds*)

The **timeout** (IP SLA) command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLA 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 79). Note that if you are configuring an IP SLAs label switched path (LSP) Health Monitor operation, see Table 80 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 **timeout** command varies depending on the Cisco IOS release you are running and the operation type configured.

If you are running Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **timeout** command.

Table 79 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Table 80 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

In the following examples, the timeout value for an IP SLAs operation 1 is set for 2500 ms:

IP SLA Configuration

```
ip sla 1
 icmp-echo 172.16.1.176
 timeout 2500
!
ip sla schedule 1 start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 timeout 2500
!
ip sla monitor schedule 1 start-time now
```

IP SLA Template Parameters Configuration

```
Router(config)#ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)#parameters
Router(config-icmp-ech-params)#timeout 2500
Router(config-icmp-ech-params)#end
Router#
00:02:26: %SYS-5-CONFIG_I: Configured from console by console
Router# show ip sla auto template type ip udp-echo
IP SLAs Auto Template: 1
    Measure Type: udp-echo (control enabled)
    Description:
.
.
.
    Operation Parameters:
        Request Data Size: 16   Verify Data: false
        Timeout: 2500 Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

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.
frequency	Sets the rate at which the IP SLAs operation restarts.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

timeout (LSP discovery)

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

timeout *seconds*

no timeout

Syntax Description

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

Command Default

5 seconds

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

tos (IP SLA)

To define a type of service (ToS) byte in the IPv4 header of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **tos** (IP SLA) command in the appropriate submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template configuration mode. To return to the default value, use the **no** form of this command.

tos *number*

no tos

Syntax Description

number	Service type byte in the IPv4 header. The range is from 0 to 255. The default is 0.

Command Default

The default type-of-service value is 0.

Command Modes

IP SLA Configuration

HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)

IP SLA Monitor Configuration

HTTP configuration (config-sla-monitor-http)
ICMP echo configuration (config-sla-monitor-echo)
ICMP path echo configuration (config-sla-monitor-pathEcho)
ICMP path jitter configuration (config-sla-monitor-pathJitter)
TCP connect configuration (config-sla-monitor-tcp)
UDP echo configuration (config-sla-monitor-udp)
UDP jitter configuration (config-sla-monitor-jitter)

IP SLA Template Configuration

ICMP echo configuration (config-tplt-icmp-ech)
ICMP jitter configuration (config-tplt-icmp-ech)
TCP connect configuration (config-tplt-tcp-conn)
UDP echo configuration (config-tplt-udp-ech)
UDP jitter configuration (config-tplt-udp-ech)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
15.1(1)T	This command was modified. The IP SLA template configuration mode was added.

Usage Guidelines

The ToS value is stored in an 8-bit field in the IPv4 packet header. This value contains information such as precedence and ToS. This information is useful for policy routing and for features like Committed Access Rate (CAR), where routers examine ToS values. This value is similar to the IPv6 traffic-class value that is stored in IPv6 packet headers using the **traffic-class** (IP SLA) command, but the two fields use different codes.

Note This command is applicable only to IPv4 networks. In an IPv6 network, use the **traffic-class** (IP SLA) command to define a traffic-class byte in the IPv6 header of a Cisco IOS IP SLAs ICMP echo operation.

When the type of service is defined for an operation, the IP SLAs Responder will reflect the ToS value it receives.

To display the ToS value for all Cisco IOS IP SLAs operations or a specified operation, use the **show ip sla configuration** command. To display the ToS value for all or an auto IP SLAs operation template, use the **show ip sla auto template** command.

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 81). 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 **tos** command varies depending on the Cisco IOS release you are running (see Table 81) and the operation type configured.

Table 81 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Examples

In the following examples, IP SLAs operation 1 is configured as an ICMP echo operation with destination IP address 172.16.1.176. The ToS value is set to 0x80. 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 81).

The examples show the **tos** (IP SLA) command being used in an IPv4 network.

IP SLA Configuration

```
ip sla 1
 icmp-echo 172.16.1.176
 tos 0x80
!
ip sla schedule 1 start-time now
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.176
 tos 0x80
!
ip sla monitor schedule 1 start-time now
```

IP SLA Template Configuration

```
Router(config)#ip sla auto template type ip udp-echo 1
Router(config-tplt-udp-ech)# source-ip 10.1.1.1
Router(config-tplt-udp-ech)# tos 80
Router(config-tplt-udp-ech# end
Router# show ip sla auto template type ip udp-echo
IP SLAs Auto Template: 1
    Measure Type: udp-echo (control enabled)
    Description:
    IP options:
        Source IP: 10.1.1.1 Source Port: 0
        VRF:    TOS: 0x80
    Operation Parameters:
        Request Data Size: 16   Verify Data: false
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
show ip sla configuration	Displays configuration values including all defaults for all Cisco IOS IP SLAs operations or a specified operation.
show ip sla auto template	Displays configuration values including all defaults for all auto IP SLAs operation templates or a specified template.
traffic-class (IP SLA)	Defines a traffic-class byte in the IPv6 header of a Cisco IOS IP SLAs ICMP echo operation in an IPv6 network.

track ip sla

To track the state of a Cisco IOS IP Service Level Agreements (SLAs) operation and to enter tracking configuration mode, use the **track ip sla** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **ip sla** *operation-number* [**state** | **reachability**]

no track *object-number* **ip sla** *operation-number* [**state** | **reachability**]

Syntax Description

object-number	Object number representing the object to be tracked. The range is from 1 to 1000.
operation-number	Number used for the identification of the IP SLAs operation you are tracking.
state	(Optional) Tracks the operation return code.
reachability	(Optional) Tracks whether the route is reachable.

Command Default

IP SLAs tracking is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced. This command replaces the **track rtr** command.
12.2(33)SXI1	This command was integrated into Cisco IOS Release 12.2(33)SXI1. This command replaces the **track rtr** command.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command replaces the **track rtr** command.
12.2(33)SRE	This command was integrated into Cisco IOS XE 12.2(33)SRE. This command replaces the **track rtr** command.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Every IP SLAs operation maintains an operation return-code value. This return code is interpreted by the tracking process. The return code may return OK, OverThreshold, and several other return codes. Different operations may have different return-code values, so only values common to all operation types are used.

Two aspects of an IP SLAs operation can be tracked: state and reachability. The difference between these aspects relates to the acceptance of the OverThreshold return code. Table 82 shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 82 Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK	Up
	(all other return codes)	Down
Reachability	OK or over threshold	Up
	(all other return codes)	Down

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
Router(config)# track 1 ip sla 2 state
```

The following example shows how to configure the tracking process to track the reachability of IP SLAs operation 3:

```
Router(config)# track 2 ip sla 3 reachability
```

Related Commands

Command	Description
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

track rtr

Note Effective with Cisco IOS Release 12.4(20)T, 12.2(33)SXI1, 12.2(33)SRE and Cisco IOS XE Release 2.4, the **track rtr** command is replaced by the **track ip sla** command. See the **track ip sla** command for more information.

To track the state of a Cisco IOS IP Service Level Agreements (SLAs) operation and to enter tracking configuration mode, use the **track rtr** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **rtr** *operation-number* {**state** | **reachability**}

no track *object-number* **rtr** *operation-number* {**state** | **reachability**}

Syntax Description

object-number	Object number representing the object to be tracked. The range is from 1 to 500.
operation-number	Number used for the identification of the IP SLAs operation you are tracking.
state	Tracks the operation return code.
reachability	Tracks whether the route is reachable.

Command Default

IP SLAs tracking is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
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(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(20)T	This command was replaced. This command was replaced by the **track ip sla** command.
12.2(33)SXI1	This command was replaced. This command was replaced by the **track ip sla** command.
Cisco IOS XE Release 2.4	This command was replaced. This command was replaced by the **track ip sla** command.
12.2(33)SRE	This command was replaced. This command was replaced by the **track ip sla** command.

Usage Guidelines

Every IP SLAs operation maintains an operation return-code value. This return code is interpreted by the tracking process. The return code may return OK, OverThreshold, and several other return codes. Different operations may have different return-code values, so only values common to all operation types are used.

Two aspects of an IP SLAs operation can be tracked: state and reachability. The difference between these aspects relates to the acceptance of the OverThreshold return code. Table 82 shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 83 Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK	Up
	(all other return codes)	Down
Reachability	OK or over threshold	Up
	(all other return codes)	Down

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
track 1 rtr 2 state
```

The following example shows how to configure the tracking process to track the reachability of IP SLAs operation 3:

```
track 2 rtr 3 reachability
```

traffic-class (IP SLA)

To define the traffic-class field in the IPv6 header of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **traffic-class** (IP SLA) 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.

traffic-class *number*

no traffic-class

Syntax Description

number	Value in the traffic-class field of the IPv6 header. The range is from 0 to 255 (or FF in hexadecimal). This value can be preceded by "0x" to indicate hexadecimal notation. The default is 0.

Defaults

The default traffic-class value is 0.

Command Modes

ICMP echo configuration (config-ip-sla-echo)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)

Note The configuration mode varies depending on the operation type configured.

Command History

Release	Modification
12.2(33)SRC	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.

Usage Guidelines

The traffic-class value is stored in an 8-bit field in the IPv6 packet header and designates the IPv6 traffic class. This field is similar to the IPv4 type-of-service (ToS) field that is configured in IPv4 packet headers using the **tos** (IP SLA) command, but the two fields use different codes.

Note The **traffic-class** command is supported only in IPv6 networks. In an IPv4 network, use the **tos** (IP SLA) command to define a ToS byte in the IPv4 header of a Cisco IOS IP SLAs operation.

When the traffic-class value is defined for an operation, the IP SLAs Responder will reflect the traffic-class value it receives.

To display the traffic class value for all Cisco IOS IP SLAs operations or a specified operation, use the **show ip sla configuration** command.

Examples

In the following example for an IPv6 network, IP SLAs operation 1 is configured as an ICMP echo operation with destination IPv6 address 2001:DB8:100::1. The value in the traffic-class field of the IPv6 header is set to 0x80.

```
ip sla 1
 icmp-echo 2001:DB8:100::1
 traffic-class 0x80
!
ip sla schedule 1 start-time now
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
show ip sla configuration	Displays configuration values including all defaults for all Cisco IOS IP SLAs operations or a specified operation.
tos (IP SLA)	Defines the ToS value in the IPv4 header of a Cisco IOS IP SLAs operation in an IPv4 network.

ttl (IP SLA)

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

ttl *time-to-live*

no ttl

Syntax Description

time-to-live	Specifies the maximum hop count for an echo request packet. For IP SLAs LSP ping operations, valid values are from 1 to 255 and the default is 255. For IP SLAs LSP traceroute operations, the range is from 1 to 30. The default is 30.

Command Default

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

Command Modes

Auto IP SLA MPLS Configuration

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

IP SLA Configuration and IP SLA Monitor Configuration

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

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see Table 84). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see Table 85 for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation.

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

Table 84 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 85 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 maximum hop count for echo request packets of IP SLAs operations created by LSP Health Monitor operation 1 is set to 200 hops.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
 ttl 200
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
```

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

Related Commands

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

type dhcp

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type dhcp** command is replaced by the **dhcp** (IP SLA) command. See the **dhcp** (IP SLA) command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Dynamic Host Configuration Protocol (DHCP) operation, use the **type dhcp** command in IP SLA monitor configuration mode.

type dhcp [**source-ipaddr** {*ip-address* | *hostname*}] [**dest-ipaddr** {*ip-address* | *hostname*}] [**option 82** [**circuit-id** *circuit-id*] [**remote-id** *remote-id*] [**subnet-mask** *subnet-mask*]]

Syntax Description

source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
dest-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the destination IP address or hostname.
option 82	(Optional) Specifies DHCP option 82 for the destination DHCP server.
circuit-id *circuit-id*	(Optional) Specifies the circuit ID in hexadecimal.
remote-id *remote-id*	(Optional) Specifies the remote ID in hexadecimal.
subnet-mask *subnet-mask*	(Optional) Specifies the subnet mask IP address. The default subnet mask is 255.255.255.0.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	The following keywords were added: • **source-ipaddr** • **dest-ipaddr** • **option 82**
12.4(4)T	This command was replaced by the **dhcp** (IP SLA) command.
12.2(33)SRB	This command was replaced by the **dhcp** (IP SLA) command.
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)SB	This command was replaced by the **dhcp** (IP SLA) command.
12.2(33)SXI	This command was replaced by the **dhcp** (IP SLA) command.

Usage Guidelines

If the source IP address is configured, then packets will be sent with that source address.

You may configure the **ip dhcp-server** global configuration command to identify the DHCP server that the DHCP operation will measure. If the target IP address is configured, then only that device will be measured. If the **ip dhcp-server** command is not configured and the target IP address is not configured, then DHCP discover packets will be sent on every available IP interface.

Option 82 is called the Relay Agent Information option and is inserted by the DHCP relay agent when client-originated DHCP packets are forwarded to a DHCP server. Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The Relay Agent Information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. The initial suboptions are defined for a relay agent that is colocated in a public circuit access unit. These suboptions are as follows: a circuit ID for the incoming circuit, a remote ID that provides a trusted identifier for the remote high-speed modem, and a subnet mask designation for the logical IP subnet from which the relay agent received the client DHCP packet.

Note If an odd number of characters are specified for the circuit ID, a zero will be added to the end of the string.

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

Examples

In the following example, IP SLAs operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3.

```
ip sla monitor 4
 type dhcp option 82 circuit-id 10005A6F1234
ip dhcp-server 172.16.20.3
!
ip sla monitor schedule 4 start-time now
```

Related Commands

Command	Description
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

type dlsw peer-ipaddr

Note Effective with Cisco IOS Releases 12.4(4)T, the **type dlsw peer-ipaddr** command is replaced by the **dlsw peer-ipaddr** command. See the **dlsw peer-ipaddr** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Data Link Switching Plus (DLSw+) operation, use the **type dlsw peer-ipaddr** command in IP SLA monitor configuration mode.

type dlsw peer-ipaddr *ip-address*

Syntax Description

ip-address	IP address of the peer destination.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	This command was replaced by the **dlsw peer-ipaddr** command.

Usage Guidelines

To configure an IP SLAs DLSw+ operation, the DLSw feature must be configured on the local and target routers.

For DLSw+ operations, the default request packet data size is 0 bytes (use the **request-data-size** command to modify this value) and the default amount of time the operation waits for a response from the request packet is 30 seconds (use the **timeout** command to modify this value).

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

Examples

In the following example, IP SLAs operation number 10 is configured as a DLSw+ operation enabled for remote peer IP address 172.21.27.11. The data size is 15 bytes.

```
ip sla monitor 10
 type dlsw peer-ipaddr 172.21.27.11
 request-data-size 15
!
ip sla monitor schedule 10 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
request-data-size	Sets the protocol data size in the payload of the IP SLAs operation's request packet.
show dlsw peers	Displays DLSw peer information.

type dns target-addr

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type dns target-addr** command is replaced by the **dns** (IP SLA) command. See the **dns** (IP SLA) command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Domain Name System (DNS) operation, use the **type dns target-addr** command in IP SLA monitor configuration mode.

type dns target-addr {*target-hostname* | *target-ip-address*} **name-server** *ip-address*
[**source-ipaddr** {*ip-address* | *hostname*} **source-port** *port-number*]

Syntax Description

target-hostname | *target-ip-address*	Target (destination) IP address or hostname.
name-server *ip-address*	Specifies the IP address of the DNS server.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	This command was replaced by the **dns** (IP SLA) command.
12.2(33)SRB	This command was replaced by the **dns** (IP SLA) command.
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)SB	This command was replaced by the **dns** (IP SLA) command.
12.2(33)SXI	This command was replaced by the **dns** (IP SLA) command.

Usage Guidelines

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

Examples

In the following example, IP SLAs operation 7 is configured as a DNS operation using the target IP address 172.20.2.132.

```
ip sla monitor 7
 type dns target-addr host1 name-server 172.20.2.132
!
ip sla monitor schedule 7 start-time now
```

Related Commands

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

type echo (MPLS)

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

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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.

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source PE router.

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

Related Commands

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

type echo domain

To configure a Cisco IOS IP Service Level Agreements (SLAs) auto Ethernet operation to create Ethernet ping operations, use the **type echo domain** command in IP SLA Ethernet monitor configuration mode.

type echo domain *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*]

Syntax Description

domain-name	Name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
evc *evc-id*	Specifies the Ethernet Virtual Circuit (EVC) identification name.
vlan *vlan-id*	Specifies the VLAN identification number.
exclude-mpids *mp-ids*	(Optional) Specifies the list of maintenance endpoint identification numbers to be excluded from the operation.

Command Default

Ethernet ping operations are not configured.

Command Modes

IP SLA Ethernet monitor (config-ip-sla-ethernet-monitor)

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)SRD	The **evc** *evc-id* keyword and argument were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

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

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

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using an IP SLAs auto Ethernet operation. In this example, operation 10 is configured to automatically create IP SLAs Ethernet ping operations for all the discovered maintenance endpoints in the domain named testdomain and VLAN identification number 34. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss events occur, a Simple Network Management Protocol (SNMP) trap notification should be sent. The schedule period for operation 10 is 60 seconds, and the operation is scheduled to start immediately.

```
ip sla ethernet-monitor 10
 type echo domain testdomain vlan 34
!
ip sla ethernet-monitor reaction-configuration 10 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
```

Related Commands

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

type echo protocol ipIcmpEcho

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type echo protocol ipIcmpEcho** command is replaced by the **icmp-echo** command. See the **icmp-echo** command for more information.

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **type echo protocol ipIcmpEcho** command in IP SLA monitor configuration mode.

type echo protocol ipIcmpEcho {*destination-ip-address* | *destination-hostname*} [**source-ipaddr** {*ip-address* | *hostname*} | **source-interface** *interface-name*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname for the operation.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-interface *interface-name*	(Optional) Specifies the source interface for the operation.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The following keyword and arguments were added: • **source-ipaddr** {*ip-address* | *hostname*}
12.3(7)XR	The **source-interface** keyword and *interface-name* argument were added.
12.3(11)T	The **source-interface** keyword and *interface-name* argument were added.
12.4(4)T	This command was replaced by the **icmp-echo** command.
12.2(33)SRB	This command was replaced by the **icmp-echo** command.
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)SB	This command was replaced by the **icmp-echo** command.
12.2(33)SXI	This command was replaced by the **icmp-echo** command.

Usage Guidelines

The default request packet data size for an ICMP echo operation is 28 bytes. Use the **request-data-size** command to modify this value. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.

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

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175.

```
ip sla monitor 10
 type echo protocol ipIcmpEcho 172.16.1.175
!
ip sla monitor schedule 10 start-time now
```

Related Commands

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

type ftp operation get url

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type ftp operation get url** command is replaced by the **ftp get** command. See the **ftp get** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) File Transfer Protocol (FTP) GET operation, use the **type ftp operation get url** command in IP SLA monitor configuration mode.

type ftp operation get url *url* [**source-ipaddr** {*ip-address* | *hostname*}] [**mode** {**passive** | **active**}]

Syntax Description

url	URL location information for the file to be retrieved.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
mode {**passive** | **active**}	(Optional) Specifies the FTP transfer mode as either passive or active. The default is passive transfer mode.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.4(4)T	This command was replaced by the **ftp get** command.
12.2(33)SRB	This command was replaced by the **ftp get** command.
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)SB	This command was replaced by the **ftp get** command.
12.2(33)SXI	This command was replaced by the **ftp get** command.

Usage Guidelines

The *url* argument must be in one of the following formats:

- ftp://username:password@host/filename
- ftp://host/filename

If the username and password are not specified, the defaults are anonymous and test, respectively.

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

Examples

In the following example, an FTP operation is configured. User1 is the username and password1 is the password; host1 is the host and file1 is the filename.

```
ip sla monitor 3
 type ftp operation get url ftp://user1:password1@host1/file1
!
ip sla monitor schedule 3 start-time now
```

Related Commands

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

type http operation

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type http operation** command is replaced by the **http** (IP SLA) command. See the **http** (IP SLA) command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) HTTP operation, use the **type http operation** command in IP SLA monitor configuration mode.

type http operation {**get** | **raw**} **url** *url* [**name-server** *ip-address*] [**version** *version-number*] [**source-ipaddr** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**cache** {**enable** | **disable**}] [**proxy** *proxy-url*]

Syntax Description

get	Specifies an HTTP GET operation.
raw	Specifies an HTTP RAW operation.
url *url*	Specifies the URL of destination HTTP server.
name-server *ip-address*	(Optional) Specifies the destination IP address of a Domain Name System (DNS) Server.
version *version-number*	(Optional) Specifies the version number.
source-ipaddr {*ip-address*| *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
cache {**enable** | **disable**}	(Optional) Enables or disables download of a cached HTTP page.
proxy *proxy-url*	(Optional) Specifies proxy information or URL.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	This command was replaced by the **http** (IP SLA) command.
12.2(33)SRB	This command was replaced by the **http** (IP SLA) command.
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)SB	This command was replaced by the **http** (IP SLA) command.
12.2(33)SXI	This command was replaced by the **http** (IP SLA) command.

Usage Guidelines

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

Examples

In the following example, IP SLAs HTTP operation 6 is configured as an HTTP RAW operation. The destination URL is http://www.cisco.com.

```
ip sla monitor 6
 type http operation raw url http://www.cisco.com
 http-raw-request
 GET /index.html HTTP/1.0\r\n
 \r\n
!
ip sla monitor schedule 6 start-time now
```

Related Commands

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

type jitter dest-ipaddr

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type jitter dest-ipaddr** command is replaced by the **udp-jitter** command. See the **udp-jitter** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation, use the **type jitter dest-ipaddr** command in IP SLA monitor configuration mode.

type jitter dest-ipaddr {*destination-ip-address* | *destination-hostname*} **dest-port** *port-number* [**source-ipaddr** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
dest-port *port-number*	Specifies the destination port number.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
control {**enable** | **disable**}	(Optional) Enables or disables the sending of IP SLAs control messages to the IP SLAs Responder. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder.
num-packets *number-of-packets*	(Optional) Number of packets, as specified by the number argument. The default value is 10.
interval *interpacket-interval*	(Optional) Interpacket interval in milliseconds. The default value is 20 ms.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	This command was replaced by the **udp-jitter** command.
12.2(33)SRB	This command was replaced by the **udp-jitter** command.
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.

Release	Modification
12.2(33)SB	This command was replaced by the **udp-jitter** command.
12.2(33)SXI	This command was replaced by the **udp-jitter** command.

Usage Guidelines

The **type jitter dest-ipaddr** command configures an IP SLAs UDP Plus operation. The UDP Plus operation is a superset of the UDP echo operation. In addition to measuring UDP round-trip time, the UDP Plus operation measures per-direction packet loss and jitter. Jitter is interpacket delay variance. Jitter statistics are useful for analyzing traffic in a Voice over IP (VoIP) network.

You must enable the IP SLAs Responder on the target router before you can configure a UDP jitter operation. Prior to sending an operation packet to the target router, IP SLAs sends a control message to the IP SLAs Responder to enable the destination port.

The default request packet data size for an IP SLAs UDP jitter operation is 32 bytes. Use the **request-data-size** command to modify this value.

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

IP SLAs VoIP UDP Jitter (codec) Operation

When you specify the codec in the command syntax of the **type jitter dest-ipaddr** command, the standard configuration options are replaced with codec-specific keywords and arguments. The codec-specific command syntax is documented separately from the command syntax for the standard implementation of the **type jitter dest-ipaddr** command. For information about the codec-specific command syntax, see the documentation for the **type jitter dest-ipaddr** (codec) command.

Examples

In the following example, operation 6 is configured as a UDP jitter operation with the destination IP address 172.30.125.15, the destination port number 2000, 20 packets, and an interpacket interval of 20 ms.

```
ip sla monitor 6
 type jitter dest-ipaddr 172.30.125.15 dest-port 2000 num-packets 20 interval 20
!
ip sla monitor schedule 6 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
request-data-size	Sets the payload size for IP SLAs operation request packets.
type jitter dest-ipaddr (codec)	Configures an IP SLAs UDP jitter operation that returns VoIP scores.

type jitter dest-ipaddr (codec)

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type jitter dest-ipaddr** (codec) command is replaced by the **udp-jitter** (codec) command. See the **udp-jitter** (codec) command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation that returns Voice over IP (VoIP) scores, use the **type jitter dest-ipaddr** command in IP SLA monitor configuration mode.

type jitter dest-ipaddr {*destination-ip-address* | *destination-hostname*} **dest-port** *port-number* **codec** *codec-type* [**codec-numpackets** *number-of-packets*] [**codec-size** *number-of-bytes*] [**codec-interval** *milliseconds*] [**advantage-factor** *value*] [**source-ipaddr** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}]

Syntax Description

destination-ip-address | *destination-hostname*	Specifies the destination IP address or hostname.
dest-port *port-number*	Specifies the destination port number. For UDP jitter (codec) operations, the port number should be an even number in the range of 16384 to 32766 or 49152 to 65534.
codec *codec-type*	Enables the generation of estimated voice-quality scores in the form of Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) values. The codec type should match the encoding algorithm you are using for VoIP transmissions. The following codec-type keywords are available: • **g711alaw**—The G.711 a-law codec (64 kbps transmission) • **g711ulaw**—The G.711 muHmm-law codec (64 kbps transmission) • **g729a**—The G.729A codec (8 kbps transmission) Configuring the codec type sets default values for the variables **codec-numpackets**, **codec-size**, and **codec-interval** in this command. See Table 86 for details.
codec-numpackets *number-of-packets*	(Optional) Specifies the number of packets to be transmitted per operation. The valid range is from 1 to 60000 packets. The default is 1000 packets.
codec-size *number-of-bytes*	(Optional) Specifies the number of bytes in each packet transmitted. (Also called the payload size or request size.) The valid range is from 16 to 1500 packets. The default varies by codec (see Table 86).
codec-interval *milliseconds*	Specifies the interval (delay) between packets that should be used for the operation, in milliseconds (ms). The valid range is from 1 to 60000 ms. By default, packets are sent 20 ms apart.
advantage-factor *value*	Specifies the expectation factor to be used for ICPIF calculations. This value is subtracted from the measured impairments to yield the final ICPIF value (and corresponding MOS value). See the "Usage Guidelines" section for recommended values. The valid range is from 0 to 20. The default is 0.

source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
control {**enable** | **disable**}	(Optional) Enables or disables the sending of IP SLAs control messages to the IP SLAs Responder. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder. **Note** Control messages are enabled by default. Disabling the IP SLAs control messages for UDP jitter operations is not recommended. If you disable IP SLAs control messages, packet loss statistics and IP telephony scores will not be generated accurately.

Defaults

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(5)T	The **type jitter dest-ipaddr** command was introduced.
12.3(4)T	The codec-specific keywords and arguments were added to the **type jitter dest-ipaddr** command to support the IP SLAs VoIP UDP jitter operation.
12.4(4)T	This command was replaced by the **udp-jitter** (codec) 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(33)SRB	This command was replaced by the **udp-jitter** (codec) command.
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)SB	This command was replaced by the **udp-jitter** (codec) command.
12.2(33)SXI	This command was replaced by the **udp-jitter** (codec) command.

Usage Guidelines

When you specify the codec in the command syntax of the **type jitter dest-ipaddr** command, the standard configuration options are replaced with codec-specific keywords and arguments. The codec-specific command syntax is documented separately from the command syntax for the standard implementation of the **type jitter dest-ipaddr** command. For information about the command syntax for the standard implementation, see the documentation for the **type jitter dest-ipaddr** command.

You must enable the IP SLAs Responder on the target router before you can configure a UDP jitter (codec) operation. Prior to sending an operation packet to the target router, IP SLAs sends a control message to the IP SLAs Responder to enable the destination port.

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

IP SLAs VoIP UDP Jitter (codec) Statistics

The IP SLAs UDP jitter operation computes statistics by sending *n* UDP packets, each of size *s*, sent *t* milliseconds apart, from a given source router to a given target router, at a given frequency *f*.

To generate MOS and ICPIF scores, you specify the codec type used for the connection when configuring the UDP jitter operation. Based on the type of codec you configure for the operation, the number of packets (*n*), the size of each payload (*s*), the inter-packet time interval (*t*), and the operational frequency (*f*) will be auto-configured with default values. (See Table 86 for specific information.) However, you are given the option, if needed, to manually configure these parameters in the syntax of the **type jitter dest-ipaddr** (codec) command.

Table 86 shows the default parameters that are configured for the operation by codec.

Table 86 Default UDP Jitter Operation Parameters by Codec

Codec	Default Number of Packets (*n*); [codec-numpackets]	Packet Payload (*s*) [codec-size][1]	Default Interval Between Packets (*t*) [codec-interval]	Frequency of Operations (*f*)
G.711 mu-law (g711ulaw)	1000	160 bytes	20 ms	Once every 60 seconds
G.711 a-law (g711alaw)	1000	160 bytes	20 ms	Once every 60 seconds
G.729A (g729a)	1000	20 bytes	20 ms	Once every 60 seconds

1. The actual data size of each request packet will contain an additional 12 bytes of Real-Time Transport Protocol (RTP) header data in order to simulate the RTP/UDP/IP/Layer 2 protocol stack.

For example, if you configure the UDP jitter operation to use the characteristics for the g711ulaw codec, by default an operation will be sent once a minute (*f*). Each operation would consist of 1000 packets (*n*), with each packet containing 160 bytes (plus 12 header bytes) of synthetic data (*s*), sent 20 ms apart (*t*).

The **advantage-factor** *value* keyword and argument allow you to specify an access Advantage Factor (also called the Expectation Factor). Table 87, adapted from ITU-T Rec. G.113, defines a set of provisional maximum values for Advantage Factors in terms of the service provided.

Table 87 Advantage Factor Recommended Maximum Values

Communication Service	Maximum Value of Advantage/ Expectation Factor (*A*):
Conventional wire line (land line)	0
Mobility (cellular connections) within a building	5

Table 87 Advantage Factor Recommended Maximum Values

Communication Service	Maximum Value of Advantage/ Expectation Factor (*A*):
Mobility within a geographical area or moving within a vehicle	10
Access to hard-to-reach location; (for example, via multihop satellite connections)	20

These values are only suggestions. To be meaningful, the use of the Advantage/Expectation factor (*A*) and its selected value in a specific application should be used consistently in any planning model you adopt. However, the values in Table 87 should be considered as the absolute upper limits for *A*. The default Advantage/Expectation factor for IP SLAs UDP jitter operations is always zero.

Examples

In the following example, IP SLAs operation 10 is configured as a UDP jitter (codec) operation with the destination IP address 209.165.200.225 and the destination port number 3000. The operation is configured to use the characteristics of the G.711 a-law codec, which means the operation will consist of 1000 packets, each of 172 bytes (160 plus 12 header bytes), sent 20 ms apart. The default value for the Advantage Factor and operation frequency is used.

```
ip sla monitor 10
 type jitter dest-ipaddr 209.165.200.225 dest-port 3000 codec g711alaw
!
ip sla monitor schedule 10 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
type jitter dest-ipaddr	Configures an IP SLAs UDP jitter operation.

type jitter domain

To configure a Cisco IOS IP Service Level Agreements (SLAs) auto Ethernet operation to create Ethernet jitter operations, use the **type jitter domain** command in IP SLA Ethernet monitor configuration mode.

type jitter domain *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} [**exclude-mpids** *mp-ids*] [**interval** *interframe-interval*] [**num-frames** *frames-number*]

Syntax Description

domain-name	Name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
evc *evc-id*	Specifies the Ethernet Virtual Circuit (EVC) identification name.
vlan *vlan-id*	Specifies the VLAN identification number.
exclude-mpids *mp-ids*	(Optional) Specifies the list of maintenance endpoint identification numbers to be excluded from the operation.
interval *interframe-interval*	(Optional) Specifies the interframe interval (in milliseconds). The default is 20.
num-frames *frames-number*	(Optional) Specifies the number of frames to be sent. The default is 10.

Command Default

Ethernet jitter operations are not configured.

Command Modes

IP SLA Ethernet monitor (config-ip-sla-ethernet-monitor)

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)SRD	The **evc** *evc-id* keyword and argument were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Note When an IP SLAs Ethernet jitter operation is created by an auto Ethernet operation, an operation number (identification number) is automatically assigned to the jitter operation. The operation numbering starts at 100001.

You must configure the type of auto Ethernet operation (such as Ethernet jitter) before you can configure any of the other parameters of the operation.

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

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using an IP SLAs auto Ethernet operation. In this example, operation 20 is configured to automatically create IP SLAs Ethernet jitter operations for all the discovered maintenance endpoints in the domain named testdomain and VLAN identification number 34. For each Ethernet jitter operation, the interframe interval is set to 20 ms and the number of frames to be sent is 30. As specified by the proactive threshold monitoring configuration, when three consecutive connection loss events occur, a Simple Network Management Protocol (SNMP) trap notification should be sent. The schedule period for operation 20 is 60 seconds, and the operation is scheduled to start immediately.

```
ip sla ethernet-monitor 20
 type jitter domain testdomain vlan 34 interval 20 num-frames 30
!
ip sla ethernet-monitor reaction-configuration 20 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
!
ip sla ethernet-monitor schedule 20 schedule-period 60 start-time now
```

Related Commands

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

type mpls lsp ping ipv4

Note Effective with Cisco IOS Release 12.2(33)SRB and 12.2(33)SB, the **type mpls lsp ping ipv4** command is replaced by the **mpls lsp ping ipv4** command. See the **mpls lsp ping ipv4** command for more information.

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

type mpls lsp ping ipv4 *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]

Syntax Description

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

Command Default

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

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	The **force-explicit-null** keyword was added.
12.2(33)SRB	This command was replaced by the **mpls lsp ping ipv4** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **mpls lsp ping ipv4** command.

Usage Guidelines

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

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

Note This command supports only single path connectivity measurements between the source PE router and associated Border Gateway Protocol (BGP) next hop neighbors.

Examples

The following examples show how to manually configure operation parameters, proactive threshold monitoring, and scheduling options for IP SLAs LSP ping operation 1.

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

Related Commands

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

type mpls lsp trace ipv4

Note Effective with Cisco IOS Release 12.2(33)SRB and 12.2(33)SB, the **type mpls lsp trace ipv4** command is replaced by the **mpls lsp trace ipv4** command. See the **mpls lsp trace ipv4** command for more information.

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

type mpls lsp trace ipv4 *destination-address destination-mask* [**force-explicit-null**] [**lsp-selector** *ip-address*] [**src-ip-addr** *source-address*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}]

Syntax Description

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

Command Default

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

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	The **force-explicit-null** keyword was added.
12.2(33)SRB	This command was replaced by the **mpls lsp trace ipv4** command.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was replaced by the **mpls lsp trace ipv4** command.

Usage Guidelines

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

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

Note This command supports only single path connectivity measurements between the source PE router and associated Border Gateway Protocol (BGP) next hop neighbors.

Examples

The following examples show how to manually configure operation parameters, proactive threshold monitoring, and scheduling options for IP SLAs LSP traceroute operation 1.

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

Related Commands

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

type pathEcho (MPLS)

To configure Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) LSP traceroute operations using the LSP Health Monitor, use the **type pathEcho** command in auto IP SLA MPLS configuration mode.

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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.

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

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

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

Examples

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

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

Related Commands

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

type pathEcho protocol ipIcmpEcho

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type pathEcho protocol ipIcmpEcho** command is replaced by the **path-echo** command. See the **path-echo** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) path echo operation, use the **type pathEcho protocol ipIcmpEcho** command in IP SLA monitor configuration mode.

type pathEcho protocol ipIcmpEcho {*destination-ip-address* | *destination-hostname*} [**source-ipaddr** {*ip-address* | *hostname*}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was replaced by the **path-echo** command.
12.2(33)SRB	This command was replaced by the **path-echo** command.
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)SB	This command was replaced by the **path-echo** command.
12.2(33)SXI	This command was replaced by the **path-echo** command.

Usage Guidelines

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

Examples

In the following example, IP SLAs operation 10 is configured as an ICMP path echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175.

```
ip sla monitor 10
 type pathEcho protocol ipIcmpEcho 172.16.1.175
!
ip sla monitor schedule 10 start-time now
```

Related Commands

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

type pathJitter dest-ipaddr

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type pathJitter dest-ipaddr** command is replaced by the **path-jitter** command. See the **path-jitter** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) path jitter operation, use the **type pathJitter dest-ipaddr** command in IP SLA monitor configuration mode.

type pathJitter dest-ipaddr {*destination-ip-address* | *destination-hostname*} [**source-ipaddr** {*ip-address* | *hostname*}] [**num-packets** *packet-number*] [**interval** *milliseconds*] [**targetOnly**]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
num-packets *packet-number*	(Optional) Specifies the number of packets to be transmitted in each operation. The default value is 10 packets per operation.
interval *milliseconds*	(Optional) Time interval between packets (in milliseconds). The default value is 20 ms.
targetOnly	(Optional) Sends test packets to the destination only (path is not traced).

Defaults

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

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.4(4)T	This command was replaced by the **path-jitter** command.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(20)S	This command was integrated into Cisco IOS Release 12.2(20)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(33)SRB	This command was replaced by the **path-jitter** command.
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)SB	This command was replaced by the **path-jitter** command.
12.2(33)SXI	This command was replaced by the **path-jitter** command.

Usage Guidelines

If the **targetOnly** keyword is used, the ICMP path jitter operation will send echoes to the destination only (the path from the source to the destination is not traced).

If the **targetOnly** keyword is not used, the IP SLAs ICMP path jitter operation will trace a "hop-by-hop" IP path from the source to the destination and then send a user-specified number of test packets to each hop along the traced path at user-specified time intervals.

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

Examples

The following example shows how to enable the ICMP path jitter operation to trace the IP path to the destination 172.69.5.6 and send 50 test packets to each hop with an interval of 30 ms between each test packet.

```
ip sla monitor 2
 type pathJitter dest-ipaddress 172.69.5.6 num-packets 50 interval 30
!
ip sla monitor schedule 2 start-time now
```

Related Commands

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

type tcpConnect dest-ipaddr

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type tcpConnect dest-ipaddr** command is replaced by the **tcp-connect** command. See the **tcp-connect** command for more information.

To define a Cisco IOS IP Service Level Agreements (SLAs) Transmission Control Protocol (TCP) connection operation, use the **type tcpConnect dest-ipaddr** command in IP SLA monitor configuration mode.

type tcpConnect dest-ipaddr {*destination-ip-address* | *destination-hostname*} **dest-port** *port-number* [**source-ipaddr** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
dest-port *port-number*	Specifies the destination port number.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
control {**enable** | **disable**}	(Optional) Enables or disables the IP SLAs control protocol to send a control message to the IP SLAs Responder prior to sending an operation packet. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder.

Defaults

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(4)T	This command was replaced by the **tcp-connect** command.
12.2(33)SRB	This command was replaced by the **tcp-connect** command.
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)SB	This command was replaced by the **tcp-connect** command.
12.2(33)SXI	This command was replaced by the **tcp-connect** command.

Usage Guidelines

The TCP connection operation is used to discover the time required to connect to the target device. This operation can be used to test virtual circuit availability or application availability. If the target is a Cisco router, then IP SLAs makes a TCP connection to any port number specified by the user. If the destination is a non-Cisco IP host, then the user must specify a known target port number (for example, 21 for FTP, 23 for Telnet, or 80 for HTTP server). This operation is useful in testing Telnet or HTTP connection times.

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

Examples

In the following example, IP SLAs operation 11 is configured as a TCP connection operation using the destination IP address 172.16.1.175 and the destination port 2400.

```
ip sla monitor 11
 type tcpConnect dest-ipaddr 172.16.1.175 dest-port 2400
!
ip sla monitor schedule 11 start-time now life forever
```

Related Commands

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

type udpEcho dest-ipaddr

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type udpEcho dest-ipaddr** command is replaced by the **udp-echo** command. See the **udp-echo** command for more information.

To define a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) echo operation, use the **type udpEcho dest-ipaddr** command in IP SLA monitor configuration mode.

type udpEcho dest-ipaddr {*ip-address* | *hostname*} **dest-port** *port-number* [**source-ipaddr** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]

Syntax Description

ip-address | *hostname*	Destination IP address or hostname of the operation.
dest-port *port-number*	Specifies the destination port number.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available UDP port.
control {**enable** | **disable**}	(Optional) Enables or disables the IP SLAs control protocol to send a control message to the IP SLAs Responder prior to sending an operation packet. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder.

Defaults

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(4)T	This command was replaced by the **udp-echo** command.
12.2(33)SRB	This command was replaced by the **udp-echo** command.
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)SB	This command was replaced by the **udp-echo** command.
12.2(33)SXI	This command was replaced by the **udp-echo** command.

Usage Guidelines

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

Examples

In the following example, IP SLAs operation 12 is configured as a UDP echo operation using the destination IP address 172.16.1.175 and destination port 2400.

```
ip sla monitor 12
 type udpEcho dest-ipaddr 172.16.1.175 dest-port 2400
!
ip sla monitor schedule 12 start-time now life forever
```

Related Commands

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

type voip delay gatekeeper registration

Note Effective with Cisco IOS Release 12.4(4)T, the **type voip delay gatekeeper registration** command is replaced by the **voip delay gatekeeper-registration** command. See the **voip delay gatekeeper-registration** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Voice over IP (VoIP) gatekeeper delay operation, use the **type voip delay gatekeeper registration** command in IP SLA monitor configuration mode.

type voip delay gatekeeper registration

Syntax Description

This command has no arguments or keywords.

Command Default

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA monitor configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **voip delay gatekeeper-registration** command.

Usage Guidelines

The IP SLAs gatekeeper registration delay operation provides statistical data on the amount of time taken to register a gateway to a gatekeeper. IP SLAs was designed to gather information over time, at intervals you specify, so that statistics can be provided on key metrics often used in Service Level Agreements (SLAs). Aggregated totals, median, or average data can be viewed using the Cisco IOS command-line interface (CLI) on the device running the IP SLAs operation, or retrieved from the device by external applications using Simple Network Management Protocol (SNMP).

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

Examples

In the following example, IP SLAs operation 10 is configured as a VoIP gatekeeper registration delay operation:

```
ip sla monitor 10
 type voip delay gatekeeper registration
!
ip sla monitor schedule 10 start-time now life forever
```

Related Commands

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

type voip delay post-dial

Note Effective with Cisco IOS Release 12.4(4)T, the **type voip delay post-dial** command is replaced by the **voip delay post-dial** command. See the **voip delay post-dial** command for more information.

To configure a Cisco IOS IP Service Level Agreements (SLAs) Voice over IP (VoIP) call setup (post-dial delay) operation, use the **type voip delay post-dial** command in IP SLA monitor configuration mode.

type voip delay post-dial [**detect-point** {**alert-ringing** | **connect-ok**}] **destination** *tag*

Syntax Description

detect-point alert-ringing	Sets the Voice over IP (VoIP) call setup operation to measure the response time for the called number to ring. If the **detect-point** keyword is not specified, the response time for the called number to ring is measured by default.
detect-point connect-ok	Sets the VoIP call setup operation to measure the response time for the called party to answer the call.
destination *tag*	Specifies the E.164 number or URL of the destination dial-peer.

Command Default

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

Command Modes

IP SLA monitor configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was replaced by the **voip delay post-dial** command.

Usage Guidelines

In order to use the IP SLAs VoIP call setup functionality, your Cisco IOS software image must support the IP SLAs VoIP test-call application and IP SLAs VoIP Responder application. To determine if your Cisco IOS software image is configured with these applications, use the **show call application voice** command in user EXEC or privileged EXEC mode.

Note The IP SLAs VoIP Responder application is different from the IP SLAs Responder (which is configured using the **ip sla monitor responder** command in global configuration mode).

If the **detect-point** keyword is not specified, the response time for the called number to ring is measured by default.

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

Examples

The following example shows how to configure an originating gateway to start the IP SLAs VoIP test-call application, set up the dial peer to route the test call, define the VoIP call setup operation, and schedule the VoIP call setup operation. In this example, test-call messages are generated using the Session Initiation Protocol (SIP).

```
call application session start ipsla-testcall ipsla-testcall
!
dial-peer voice 6789 voip
destination-pattern 6789
session target ipv4:172.29.129.123
session protocol sipv2
!
ip sla monitor 1
 type voip delay post-dial detect-point alert-ringing destination 6789
!
ip sla monitor schedule 1 start-time now life forever
```

The following example shows how to configure a terminating gateway to set up the dial peer and enable the IP SLAs VoIP Responder application to respond to the IP SLAs VoIP call setup test call. In this example, test-call messages are generated using the Session Initiation Protocol (SIP).

```
dial-peer voice 6789 voip
incoming called-number 6789
application ipsla-responder
session protocol sipv2
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
show call application voice	Displays information about configured voice applications.

udp-echo

To define a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) echo operation, use the **udp-echo** command in IP SLA configuration mode.

udp-echo {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname of the operation.
destination-port	Specifies the destination port number.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available UDP port.
control {**enable** | **disable**}	(Optional) Enables or disables the IP SLAs control protocol to send a control message to the IP SLAs Responder prior to sending an operation packet. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder.

Defaults

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type udpEcho dest-ipaddr** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type udpEcho dest-ipaddr** command.
12.2(33)SRC	Support for IPv6 addresses was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type udpEcho dest-ipaddr** command. Support for IPv6 addresses was added.
12.4(20)T	Support for IPv6 addresses was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type udpEcho dest-ipaddr** command.

Usage Guidelines

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

IP SLAs UDP echo operations support both IPv4 and IPv6 addresses.

Control protocol is required when the target device is a Cisco router that does not natively provide the UDP or TCP Connect service. If you disable control by using the **control disable** keyword combination, you must define the IP address of the source for the Cisco IOS IP SLAs Responder by using the **ip sla responder udp-echo ipaddress** command on the destination device.

Examples

In the following example, IP SLAs operation 12 is configured as a UDP echo operation using the destination IPv4 address 172.16.1.175 and destination port 2400:

```
ip sla 12
 udp-echo 172.16.1.175 2400
!
ip sla schedule 12 start-time now life forever
```

In the following example, IP SLAs operation 13 is configured as a UDP echo operation using the destination IPv6 address 2001:DB8:100::1 and destination port 2400:

```
ip sla 13
 udp-echo 2001:DB8:100::1 2400
!
ip sla schedule 13 start-time now life forever
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla responder udp-echo ipaddress	Permanently enables IP SLAs Responder functionality on specified IP address and port.

udp-jitter

To configure a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation, use the **udp-jitter** command in IP SLA configuration mode.

udp-jitter {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname.
destination-port	Specifies the destination port number.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
control {**enable** | **disable**}	(Optional) Enables or disables the sending of IP SLAs control messages to the IP SLAs Responder. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder.
num-packets *number-of-packets*	(Optional) Number of packets, as specified by the number argument. The default is 10.
interval *interpacket-interval*	(Optional) Interpacket interval in milliseconds. The default is 20.

Defaults

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type jitter dest-ipaddr** command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB. This command replaces the **type jitter dest-ipaddr** command.
12.2(33)SRC	Support for IPv6 addresses was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type jitter dest-ipaddr** command. Support for IPv6 addresses was added.

12.4(20)T	Support for IPv6 addresses was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type jitter dest-ipaddr** command.

Usage Guidelines

The **udp-jitter** command configures an IP SLAs UDP Plus operation. The UDP Plus operation is a superset of the UDP echo operation. In addition to measuring UDP round-trip time, the UDP Plus operation measures per-direction packet loss and jitter. Jitter is interpacket delay variance. Jitter statistics are useful for analyzing traffic in a Voice over IP (VoIP) network.

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

You must enable the IP SLAs Responder on the target router before you can configure a UDP jitter operation. Prior to sending an operation packet to the target router, IP SLAs sends a control message to the IP SLAs Responder to enable the destination port. Control protocol is required when the target device is a Cisco router that does not natively provide the UDP or TCP Connect service. If you disable control by using the **control disable** keyword combination with this command, you must define the IP address of the source for the Cisco IOS IP SLAs Responder by using the **ip sla responder udp-echo ipaddress** command on the destination device.

The default request packet data size for an IP SLAs UDP jitter operation is 32 bytes. Use the **request-data-size** command to modify this value.

IP SLAs UDP jitter operations support both IPv4 and IPv6 addresses.

IP SLAs VoIP UDP Jitter (codec) Operation

When you specify the codec in the command syntax of the **udp-jitter** command, the standard configuration options are replaced with codec-specific keywords and arguments. The codec-specific command syntax is documented separately from the command syntax for the standard implementation of the **udp-jitter** command. For information about the codec-specific command syntax, see the documentation for the **udp-jitter** (codec) command.

Examples

In the following example, operation 6 is configured as a UDP jitter operation with the destination IPv4 address 172.30.125.15, the destination port number 2000, 20 packets, and an interpacket interval of 20 ms:

```
ip sla 6
 udp-jitter 172.30.125.15 2000 num-packets 20 interval 20
!
ip sla schedule 6 start-time now
```

In the following example, operation 7 is configured as a UDP jitter operation with the destination IPv6 address 2001:0DB8:200::FFFE, the destination port number 2000, 20 packets, and an interpacket interval of 20 ms:

```
ip sla 7
 udp-jitter 2001:0DB8:200::FFFE 2000 num-packets 20 interval 20
!
ip sla schedule 7 start-time now
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla responder udp-echo ipaddress	Permanently enables IP SLAs Responder functionality on specified IP address and port.
request-data-size	Sets the payload size for IP SLAs operation request packets.
udp-jitter (codec)	Configures an IP SLAs UDP jitter operation that returns VoIP scores.

udp-jitter (codec)

To configure a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation that returns Voice over IP (VoIP) scores, use the **udp-jitter** command in IP SLA configuration mode.

udp-jitter {*destination-ip-address* | *destination-hostname*} *destination-port* **codec** *codec-type* [**codec-numpackets** *number-of-packets*] [**codec-size** *number-of-bytes*] [**codec-interval** *milliseconds*] [**advantage-factor** *value*] [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}]

Syntax Description

destination-ip-address | *destination-hostname*	Specifies the destination IP address or hostname.
destination-port	Specifies the destination port number. For UDP jitter (codec) operations, the port number should be an even number in the range of 16384 to 32766 or 49152 to 65534.
codec *codec-type*	Enables the generation of estimated voice-quality scores in the form of Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) values. The codec type should match the encoding algorithm you are using for VoIP transmissions. The following codec-type keywords are available: • **g711alaw**—The G.711 a-law codec (64 kbps transmission) • **g711ulaw**—The G.711 muHmm-law codec (64 kbps transmission) • **g729a**—The G.729A codec (8 kbps transmission) Configuring the codec type sets default values for the variables **codec-numpackets**, **codec-size**, and **codec-interval** in this command. See Table 88 for details.
codec-numpackets *number-of-packets*	(Optional) Specifies the number of packets to be transmitted per operation. The range is from 1 to 60000. The default is 1000.
codec-size *number-of-bytes*	(Optional) Specifies the number of bytes in each packet transmitted. (Also called the payload size or request size.) The range is from 16 to 1500. The default varies by codec (see Table 88).
codec-interval *milliseconds*	Specifies the interval (delay) between packets that should be used for the operation, in milliseconds (ms). The range is from 1 to 60000. The default is 20.
advantage-factor *value*	Specifies the expectation factor to be used for ICPIF calculations. This value is subtracted from the measured impairments to yield the final ICPIF value (and corresponding MOS value). See the "Usage Guidelines" section for recommended values. The range is from 0 to 20. The default is 0.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.

source-port *port-number*	(Optional) Specifies the source port number. When a port number is not specified, IP SLAs chooses an available port.
control {**enable** | **disable**}	(Optional) Enables or disables the sending of IP SLAs control messages to the IP SLAs Responder. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs Responder. **Note** Control messages are enabled by default. Disabling the IP SLAs control messages for UDP jitter operations is not recommended. If you disable IP SLAs control messages, packet loss statistics and IP telephony scores will not be generated accurately.

Defaults

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type jitter dest-ipaddr** (codec) command.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB**.** This command replaces the **type jitter dest-ipaddr** (codec) command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command replaces the **type jitter dest-ipaddr** (codec) command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **type jitter dest-ipaddr** (codec) command.

Usage Guidelines

When you specify the codec in the command syntax of the **udp-jitter** command, the standard configuration options are replaced with codec-specific keywords and arguments. The codec-specific command syntax is documented separately from the command syntax for the standard implementation of the **udp-jitter** command. For information about the command syntax for the standard implementation, see the documentation for the **udp-jitter** command.

You must enable the IP SLAs Responder on the target router before you can configure a UDP jitter (codec) operation. Prior to sending an operation packet to the target router, IP SLAs sends a control message to the IP SLAs Responder to enable the destination port.

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

IP SLAs VoIP UDP Jitter (codec) Statistics

The IP SLAs UDP jitter operation computes statistics by sending *n* UDP packets, each of size *s*, sent *t* milliseconds apart, from a given source router to a given target router, at a given frequency *f*.

To generate MOS and ICPIF scores, you specify the codec type used for the connection when configuring the UDP jitter operation. Based on the type of codec you configure for the operation, the number of packets (*n*), the size of each payload (*s*), the inter-packet time interval (*t*), and the operational frequency (*f*) will be auto-configured with default values. (See Table 88 for specific information.) However, you are given the option, if needed, to manually configure these parameters in the syntax of the **udp-jitter** (codec) command.

Table 88 shows the default parameters that are configured for the operation by codec.

Table 88 Default UDP Jitter Operation Parameters by Codec

Codec	Default Number of Packets (*n*); [codec-numpackets]	Packet Payload (*s*) [codec-size][1]	Default Interval Between Packets (*t*) [codec-interval]	Frequency of Operations (*f*)
G.711 mu-law (g711ulaw)	1000	160 bytes	20 ms	Once every 60 seconds
G.711 a-law (g711alaw)	1000	160 bytes	20 ms	Once every 60 seconds
G.729A (g729a)	1000	20 bytes	20 ms	Once every 60 seconds

1. The actual data size of each request packet will contain an additional 12 bytes of Real-Time Transport Protocol (RTP) header data in order to simulate the RTP/UDP/IP/Layer 2 protocol stack.

For example, if you configure the UDP jitter operation to use the characteristics for the g711ulaw codec, by default an operation will be sent once a minute (*f*). Each operation would consist of 1000 packets (*n*), with each packet containing 160 bytes (plus 12 header bytes) of synthetic data (*s*), sent 20 ms apart (*t*).

The **advantage-factor** *value* keyword and argument allow you to specify an access Advantage Factor (also called the Expectation Factor). Table 89, adapted from ITU-T Rec. G.113, defines a set of provisional maximum values for Advantage Factors in terms of the service provided.

Table 89 Advantage Factor Recommended Maximum Values

Communication Service	Maximum Value of Advantage/ Expectation Factor (*A*):
Conventional wire line (land line)	0
Mobility (cellular connections) within a building	5
Mobility within a geographical area or moving within a vehicle	10
Access to hard-to-reach location; (for example, via multihop satellite connections)	20

These values are only suggestions. To be meaningful, the use of the Advantage/Expectation factor (*A*) and its selected value in a specific application should be used consistently in any planning model you adopt. However, the values in Table 89 should be considered as the absolute upper limits for *A*. The default Advantage/Expectation factor for IP SLAs UDP jitter operations is always zero.

Examples

In the following example, IP SLAs operation 10 is configured as a UDP jitter (codec) operation with the destination IP address 209.165.200.225 and the destination port number 3000. The operation is configured to use the characteristics of the G.711 a-law codec, which means the operation will consist of 1000 packets, each of 172 bytes (160 plus 12 header bytes), sent 20 ms apart. The default value for the Advantage Factor and operations frequency is used.

```
ip sla 10
 udp-jitter 209.165.200.225 3000 codec g711alaw
!
ip sla schedule 10 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
udp-jitter	Configures an IP SLAs UDP jitter operation.

verify-data (IP SLA)

To cause a Cisco IOS IP Service Level Agreements (SLAs) operation to check each reply packet for data corruption, use the **verify-data** (IP SLA) command in the appropriate submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

verify-data

no verify-data

Syntax Description

This command has no arguments or keywords.

Command Default

Data is not checked for corruption.

Command Modes

IP SLA Configuration

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)

IP SLA Monitor Configuration

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)

IP SLA Template Parameters Configuration

ICMP echo configuration (config-icmp-ech-params)
UDP echo configuration (config-udp-ech-params)
UDP jitter configuration (config-udp-jtr-params)

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.
15.1(1)T	This command was modified. The IP SLA template parameters configuration mode was added.

Usage Guidelines

Use the **verify-data** (IP SLA) command only when data corruption may be an issue. Do not enable this feature during normal operation because it can cause unnecessary network overhead.

The **verify-data** command is supported in IPv4 networks. This command can also be used 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 90). 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 **verify-data** (IP SLA) command varies depending on the Cisco IOS release you are running (see Table 90) and the operation type configured.

If you are running Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **verify-data** command.

Table 90 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Examples

The following examples show how to configure an IP SLAs ICMP echo operation to verify each reply packet for data corruption. 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 90).

IP SLA Configuration

```
ip sla 5
 icmp-echo 172.16.1.174
 verify-data
!
ip sla schedule 5 start-time now life forever
```

IP SLA Monitor Configuration

```
ip sla monitor 5
 type echo protocol ipIcmpEcho 172.16.1.174
 verify-data
!
ip sla monitor schedule 5 start-time now life forever
```

IP SLA Template Configuration

```
Router(config)#ip sla auto template type ip icmp-echo 5
Router(config-tplt-icmp-ech)#parameters
Router(config-icmp-ech-params)#verify-data
Router(config-icmp-ech-params)#end
Router#
```

```
00:02:26: %SYS-5-CONFIG_I: Configured from console by console
Router# show ip sla auto template type ip icmp-echo 5
IP SLAs Auto Template: 5
    Measure Type: icmp-echo
    Description:
.
.
.
Operation Parameters:
        Request Data Size: 28   Verify Data: true
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

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

voip delay gatekeeper-registration

To configure a Cisco IOS IP Service Level Agreements (SLAs) Voice over IP (VoIP) gatekeeper delay operation, use the **voip delay gatekeeper-registration** command in IP SLA configuration mode.

voip delay gatekeeper-registration

Syntax Description

This command has no arguments or keywords.

Command Default

No IP SLAs operation type is associated with the operation number being configured.

Command Modes

IP SLA configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type voip delay gatekeeper registration** command.

Usage Guidelines

The IP SLAs gatekeeper registration delay operation provides statistical data on the amount of time taken to register a gateway to a gatekeeper. IP SLAs was designed to gather information over time, at intervals you specify, so that statistics can be provided on key metrics often used in Service Level Agreements (SLAs). Aggregated totals, median, or average data can be viewed using the Cisco IOS command-line interface (CLI) on the device running the IP SLAs operation, or retrieved from the device by external applications using Simple Network Management Protocol (SNMP).

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

Examples

In the following example, IP SLAs operation 10 is configured as a VoIP gatekeeper registration delay operation:

```
ip sla 10
 voip delay gatekeeper-registration
!
ip sla schedule 10 start-time now life forever
```

Related Commands

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

voip delay post-dial

To configure a Cisco IOS IP Service Level Agreements (SLAs) Voice over IP (VoIP) call setup (post-dial delay) operation, use the **voip delay post-dial** command in IP SLA configuration mode.

voip delay post-dial [**detect-point** {**alert-ringing** | **connect-ok**}] **destination** *tag*

Syntax Description

detect-point alert-ringing	Sets the Voice over IP (VoIP) call setup operation to measure the response time for the called number to ring. If the **detect-point** keyword is not specified, the response time for the called number to ring is measured by default.
detect-point connect-ok	Sets the VoIP call setup operation to measure the response time for the called party to answer the call.
destination *tag*	Specifies the E.164 number or URL of the destination dial-peer.

Command Default

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

Command Modes

IP SLA configuration

Command History

Release	Modification
12.4(4)T	This command was introduced. This command replaces the **type voip delay post-dial** command.

Usage Guidelines

In order to use the IP SLAs VoIP call setup functionality, your Cisco IOS software image must support the IP SLAs VoIP test-call application and IP SLAs VoIP Responder application. To determine if your Cisco IOS software image is configured with these applications, use the **show call application voice** command in user EXEC or privileged EXEC mode.

Note The IP SLAs VoIP Responder application is different from the IP SLAs Responder (which is configured using the **ip sla responder** command in global configuration mode).

If the **detect-point** keyword is not specified, the response time for the called number to ring is measured by default.

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

Examples

The following example shows how to configure an originating gateway to start the IP SLAs VoIP test-call application, set up the dial peer to route the test call, define the VoIP call setup operation, and schedule the VoIP call setup operation. In this example, test-call messages are generated using the Session Initiation Protocol (SIP).

```
call application session start ipsla-testcall ipsla-testcall
!
dial-peer voice 6789 voip
destination-pattern 6789
session target ipv4:172.29.129.123
session protocol sipv2
!
ip sla 1
 voip delay post-dial detect-point alert-ringing destination 6789
!
ip sla schedule 1 start-time now life forever
```

The following example shows how to configure a terminating gateway to set up the dial peer and enable the IP SLAs VoIP Responder application to respond to the IP SLAs VoIP call setup test call. In this example, test-call messages are generated using the Session Initiation Protocol (SIP).

```
dial-peer voice 6789 voip
incoming called-number 6789
application ipsla-responder
session protocol sipv2
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
show call application voice	Displays information about configured voice applications.

voip rtp

To configure a Cisco IOS IP Service Level Agreement (SLAs) RTP-based Voice over IP (VoIP) operation, use the **voip rtp** command in IP SLA configuration mode.

voip rtp {*destination-ip-address* | *destination-hostname*} **source-ip** {*ip-address* | *hostname*} **source-voice-port** {*slot* [*/subunit/port*:*ds0-group-number*]} [**codec** *codec-type*] [**duration** *seconds*] [**advantage-factor** *value*]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname.
source-ip {*ip-address* | *hostname*}	Specifies the source IP address or hostname.
source-voice-port	Specifies the source voice port.
slot	Source slot number.
/subunit	Source subunit number. A slash must precede this value.
/port	Source port number. A slash must precede this value.
:*ds0-group-number*	Source DS0 group number. A colon must precede this value.
codec *codec-type*	(Optional) Enables the generation of estimated voice quality scores in the form of Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) values. The codec type should match the encoding algorithm you are using for VoIP transmissions. The following codec type keywords are available: • **g711alaw**—The G.711 A-Law codec (64 kbps transmission) • **g711ulaw**—The G.711 muHmm-Law codec (64 kbps transmission) • **g729a**—The G.729A codec (8 kbps transmission) Default codec type is the G.729A codec.
duration *seconds*	(Optional) Specifies the duration (in seconds) of the test call. The default is 20 seconds.
advantage-factor *value*	(Optional) Specifies the expectation factor to be used for ICPIF calculations. This value is subtracted from the measured impairments to yield the final ICPIF value (and corresponding MOS value). The valid range is from 0 to 20. The default is 0.

Command Default

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

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure an IP SLAs RTP-based VoIP operation:

```
ip sla 1
 voip rtp 10.2.3.4 source-ip 10.5.6.7 source-voice-port 1/0:1 codec g711alaw duration 30
advantage-factor 5
 exit
!
ip sla reaction-configuration 1 react FrameLossDS threshold-type consecutive 3 action-type
traponly
!
ip sla schedule 1 start-time now life forever
```

Related Commands

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

vrf (IP SLA)

To allow monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using Cisco IOS IP Service Level Agreements (SLAs) operations, use the **vrf** command in the appropriate submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template configuration mode.

vrf *vrf-name*

Syntax Description

vrf-name	VPN routing and forwarding (VRF) name.

Command Default

The MPLS VPN parameter is not configured for the IP SLAs operation.

Command Modes

IP SLA Configuration

DNS configuration (config-ip-sla-dns)
FTP configuration (config-ip-sla-ftp)
HTTP configuration (config-ip-sla-http)
ICMP echo configuration (config-ip-sla-echo)
ICMP jitter configuration (config-ip-sla-icmpjitter)
ICMP path echo configuration (config-ip-sla-pathEcho)
ICMP path jitter configuration (config-ip-sla-pathJitter)
TCP connect configuration (config-ip-sla-tcp)
UDP echo configuration (config-ip-sla-udp)
UDP jitter configuration (config-ip-sla-jitter)

IP SLA Monitor Configuration

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)

IP SLA Template Configuration

ICMP echo configuration (config-tplt-icmp-ech)
ICMP jitter configuration (config-tplt-icmp-ech)
TCP connect configuration (config-tplt-tcp-conn)
UDP echo configuration (config-tplt-udp-ech)
UDP jitter configuration (config-tplt-udp-ech)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(11)T	Syntax changed from **vrfName** to **vrf** with SAA Engine II.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S. Support for this command was also added for ICMP path jitter operations.

Release	Modification
12.3(2)T	Support for this command was added for ICMP path jitter operations.
12.2(20)S	This command was integrated into Cisco IOS Release 12.2(20)S. Support for this command was also added for ICMP path jitter operations.
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.
12.2SX	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.
12.4(20)T	Support for this command was added for the IP SLAs DNS, FTP, HTTP, and TCP connect operations.
15.1(1)T	This command was modified. The IP SLA template configuration mode was added.

Usage Guidelines

This command identifies the VPN for the operation being configured.

Use this command only if the response time over the VPN tunnel must be measured.

For ICMP path jitter operations, you must specify the source IP address or hostname when using the **vrf** command.

The **vrf** (IP SLA) command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure 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 91). 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 **vrf** (IP SLA) command varies depending on the Cisco IOS release you are running (see Table 91) and the operation type configured.

Table 91 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
15.1(1)T	**ip sla auto template**	IP SLA template configuration

Examples

The following examples show how to configure an IP SLAs operation for an MPLS VPN. These examples show how test traffic can be sent in an already existing VPN tunnel between two endpoints.

IP SLA Configuration

```
ip sla 1
 icmp-echo 10.1.1.1
 vrf vpn1
!
ip sla schedule 1 start now
```

IP SLA Monitor Configuration

```
ip sla monitor 1
 type echo protocol ipIcmpEcho 10.1.1.1
 vrf vpn1
!
ip sla monitor schedule 1 start now
```

IP SLA Template Configuration

```
Router(config)#ip sla auto template type ip icmp-echo 1
Router(config-tplt-icmp-ech)#source-ip 10.1.1.1
Router(config-tplt-icmp-ech)#vrf vpn1
Router(config-icmp-ech-params)#end
Router#
00:02:26: %SYS-5-CONFIG_I: Configured from console by console
Router# show ip sla auto template type ip icmp-echo 1
IP SLAs Auto Template: 1
    Measure Type: icmp-echo
    Description:
    IP options:
        Source IP: 10.1.1.1
        VRF: vpn1       TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

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