I through P

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-addressdestination-hostname* [**source-ip** *ip-addresshostname* | **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 IP v4 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.

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. 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-addressdestination-hostname* [**interval** *milliseconds*] [**num-packets** *packet-number*] [**source-ip** *ip-addresshostname*]

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.

inner-cos

To set the class of service (CoS) for the inner loop in a service performance packet profile, use the **inner-cos** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

inner-cos *cos-number*

Syntax Description

cos-number	Class of service (CoS) value. The range is from 0 to 7.

Command Default

No CoS number for the inner loop is configured in the packet profile.

Command Modes

Packet profile submode of IP SLA service performance configuration (config-ip-sla-service-packet)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
.
.
.

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
.
.
.
```

Related Commands

Command	Description
profile packet	Creates a packet profile for live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

inner-eth-type

To set the encapsulation type for the inner VLAN tag of the interface from which the message will be sent, use the **inner-eth-type** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

inner-eth-type { dot1ad | dot1q }

Command Default

If you do not specify encapsulation type in the packet profile, it is considered as dot1q encapsulation.

Command Modes

Packet profile submode of IP SLA service performance configuration (config-ip-sla-service-performance-packet)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 0010.0010.0010
.
.
.

Profile Traffic:
Direction: internal
CIR: 10000
EIR: 20000
CBS: 0
EBS: 0
Burst Size: 0
Burst Duration: 0
Inter Burst Interval: 0
Rate Step (kbps): 30000
Mode: conform-color
Action: Transmit
Set COS: 2
Mode: exceed-color
Action: Transmit
Set COS: 7
Mode:
Action: Transmit
Set COS: 0
Set Tunnel EXP: 0

Profile Packet[0] :
Inner COS: Not Set
Outer COS: 3
Inner VLAN: Not Set
Outer VLAN: 100
DSCP: default
```

```
Packet Size: 1024
Source MAC Address: 0020.0020.0020
EtherType: default
outer-eth-type: dot1q
inner-eth-type: dot1q

Number of Packets: 100
.
.
.
```

Related Commands

Command	Description
outer-eth-type	Sets the encapsulation type that will be populated in the outer VLAN tag of the packet.

inner-vlan

To specify a VLAN for the inner loop in a service performance packet profile, use the **inner-vlan** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

inner-vlan *vlan-id*
no inner-vlan

Syntax Description

vlan	VLAN identifier. The range is from 0 to 4096.

Command Default

No VLAN for the inner loop is configured in the packet profile.

Command Modes

Packet profile submode of IP SLA service performance configuration (config-ip-sla-service-packet)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
.
.
.

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
.
.
.
```

Related Commands

Command	Description
profile packet	Creates a packet profile for live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

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 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	IP 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. **Note** The port configuration is required but ignored by a multicast UDP jitter operation.

Command Default

The 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.
15.2(3)T	This command was modified. Support was added for IPv6.
15.2(4)M	This command was modified. Support was added for configuring a list of unicast IP addresses for multicast UDP jitter operations.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

This command adds IPv4 or IPv6 addresses to the 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 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 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.

Use the **endpoint-list** keyword with the **udp-jitter** command to specify an endpoint list for a multicast UDP jitter operation.

Examples

Note In Cisco IOS Release 15.2(3)T, the **ip sla auto endpoint-list** command was replaced by the **ip sla endpoint-list** command and the **show ip sla auto endpoint-list** command was replaced by the **show ip sla endpoint-list** command.

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

```
Router(config)#ip sla 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-list** command shows the results of the preceding configuration. If this list is for a multicast UDP jitter operation, the port configuration is ignored by the operation.

```
Router# show ip sla 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.

Command	Description
show ip sla auto endpoint-list	Displays configuration including default values of IP SLAs endpoint lists.
show ip sla endpoint-list	(For Cisco IOS Release 15.2(3)T and later releases) Displays configuration including default values of IP SLAs endpoint lists.
udp-jitter	Configures an IP SLAs multicast UDP jitter operation.

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.

Command Default

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.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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.

Command	Description
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

Note Effective with Cisco IOS Release 15.2(3)T, the **ip sla auto endpoint-list** command is replaced with the **ip sla endpoint-list** command. See the **ip sla endpoint-list** command for more information.

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.
15.2(3)T	This command was replaced by the **ip sla endpoint-list** command.

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 enable timestamp

To enable low-level time stamping for IP Service Level Agreements (SLAs), use the **ip sla enable timestamp** command in global configuration mode. To return to the default, use the **no** form of this command.

ip sla enable timestamp
no ip sla enable timestamp

Syntax Description

This command has no arguments or keywords.

Command Default

Low-level time stamping is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(53)SE	This command was introduced.

Usage Guidelines

Use the **ip sla enable timestamp** command to enable low-level time stamping for IP SLAs.

IP SLAs low-level time stamping increases the length of time between when the packet arrives at the interface and when the packet is handed to the application. For Hot Standby Router Protocol (HSRP) on a Cisco Catalyst 3560 Series switch, the longer elapsed time will exceed the default hold time at the standby interface, causing the standby HSRP to be declared active and making both (the active and standby) HSRPs active at the same time. To ensure that HSRP continues to operate correctly when the IP SLAs time stamp is enabled, also configure the **standby timers** command on the standby interface to increase the HSRP hello and hold timers. The recommended hello and hold timer values are 15 seconds and 16 seconds, respectively.

Examples

```
!
interface FastEthernet0
 standby ip 172.19.10.1
 standby 0 timers 15 16
.
.
.

ip sla enable timestamp
ip sla enable reaction-alerts
```

Related Commands

Command	Description
standby timers	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.

ip sla endpoint-list

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

ip sla endpoint-list type ip | ipv6 *template-name*
no ip | ipv6 sla endpoint-list *template-name*

Syntax Description

type ip	Specifies that the operation type is IPv4.
type ipv6	Specifies that the operation type is IPv6.
template-name	Unique identifier of the endpoint list. Length of string is 1 to 64 ASCII characters.

Command Default

No IP SLAs endpoint list is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(3)T	This command was introduced. This command replaced the **ip sla auto endpoint-list** command.

Usage Guidelines

This command assigns a name to an 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 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 IP SLAs endpoint lists of endpoints, one by manually configuring destination IP addresses and one using auto discovery:

```
Router(config)# ip sla 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 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 endpoint-list	Displays configuration including default values of IP SLAs endpoint lists.

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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

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 **ipslaethernet-monitorreaction-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-typenever** 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-typenever** 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 **reactrttthreshold-typeaverage3** 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-valuey-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 (**xofy55**). The valid range for each value is from 1 to 16.
threshold-value [*upper-thresholdlower-threshold*]	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See the table 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 **ipslaethernet-monitorreaction-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 **noipslaethernet-monitorreaction-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 **ipslaloggingtraps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-serverenabletrapsrtr** 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 **showipslaethernet-monitorconfiguration** command.

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 1: 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.

Command	Description
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.

Release	Modification
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* | **schedule-together** [**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* | **random** *milliseconds*]
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 15.2(4)T and later releases and in Cisco IOS Release 15.1(1)T: 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.
schedule-together	Starts and runs all of the specified operations at the same time.
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.
random *milliseconds*	(Optional) Adds a random number of milliseconds (between 0 and the specified value) to the current time, after which the operation will start. The range is from 0 to 10000.

Command Default

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.
15.1(4)M	This command was modified. A random scheduler will not schedule an IP SLAs probe for which enhanced-history is configured. A fixed frequency multioperation scheduler will not schedule an IP SLAs probe for which enhanced history is configured if the enhanced-history interval is not a multiple of the scheduler frequency.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.2(4)T	This command was modified. Support for scheduling a single operation was added.
15.3(1)T	This command was modified. The **random** keyword was added for scheduling a random start time.
15.3(2)S	This command was modified. The **schedule-together** keyword was added. This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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 cancelling. 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.

Use the **random** keyword with the **start-time** keyword to randomly choose a scheduled start time for the operation. A random number of milliseconds between 0 and the specified value will be added to the current time to define the start time. The value provided for the random start time applies only to the first time the operation runs after which normal frequency rules apply.

In Cisco IOS Release 15.2(4)T and later releases, and in Cisco IOS Release 15.1(1)T, a single operation ID is a valid option for the *operation-ids* argument. Before Cisco IOS Release 15.1(1)T and in releases between Cisco IOS Release 15.1(1)T and 15.2(4)T, the **ip sla group schedule** command was not 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
```

Before Cisco IOS Release 15.1(4)M, if an IP SLAs probe that included the **history enhanced** command was added to a multioperation scheduler and the enhanced-history interval was not a multiple of the scheduler frequency, the enhanced-history interval was overwritten and set to a multiple of the scheduler frequency.

In Cisco IOS Release 15.1(4)M and later releases, if an IP SLAs probe that includes the **history enhanced** command is added to a multioperation scheduler and the enhanced-history interval is not a multiple of the scheduler frequency, the probe is not scheduled and the following message is displayed:

```
Warning, some probes not scheduled because they have Enhanced History Interval which not
multiple of group frequency.
```

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.
- Before Cisco IOS Release 15.1(4)M, if an IP SLAs probe that includes the **history enhanced** command is added to a random scheduler, the probe may or may not be scheduled.
- In Cisco IOS Release 15.1(4)M and later releases, if an IP SLAs probe that includes the **history enhanced** command is added to a random scheduler, the probe is not scheduled and the following message is displayed:

  ```
  Warning, some probes not scheduled because they have Enhanced History configured.
  ```

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.

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.

Command Default

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.

Command Default

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.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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.

Command Default

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.

Command Default

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.

Command Default

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 cancelling. 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.

Command Default

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.

Command Default

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.

Command Default

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 **ipslamonitorreaction-configuration**command is replaced by the **ipslareaction-configuration**command. See the **ipslareaction-configuration**command for more information.

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **ipslamonitorreaction-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-typenever**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 **ipslamonitorreaction-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 **reactrttthreshold-typeaverage3** 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 **showipslamonitorreaction-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-valuey-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 (**xofy55**). The valid range for each value is from 1 to 16. The *x-value* will appear in the output of the **showipslamonitorreaction-configuration** command as the “Threshold Count” value, and the *y-value* will appear as the “Threshold Count2” value.
[**threshold-value***upper-thresholdlower-threshold*]	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See the table in the “Usage Guidelines” section for a list of the default values. **Note** For MOS threshold values (**reactmos**), 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.

Note See the table 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 **ipslareaction-configuration**command.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command replaces the **rtrreaction-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 **ipslareaction-configuration**command.
12.2(33)SXI	This command was replaced by the **ipslareaction-configuration**command.

Usage Guidelines

You can configure the **ipslamonitorreaction-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 **noipslamonitorreaction-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 **ipslamonitorloggingtraps**command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-serverenabletrapsrtr** 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 **showipslamonitorconfiguration** command.

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 2: Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms

Monitored Element Keyword	Upper Threshold	Lower Threshold
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 **ipslamonitorreaction-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** globalconfiguration command).
target-operation	Number of the operation that will be triggered into an active state.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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 on-demand ethernet

To configure an on-demand IP Service Level Agreements (SLAs) IP SLAs Metro-Ethernet 3.0 delay, delay variation, or loss operation for real-time troubleshooting of Ethernet services, use the **ip sla on-demand ethernet** command in privileged EXEC mode.

ip sla on-demand ethernetDMMv1 | **SLM** *operation-number* | **domain** *domain-name* **evc** *evc-id* | **vlan** *vlan-id* **mpid** *target-mp-id* | **mac-address** *target-address* **cos** *cos* **source mpid** *source-mp-id* | **mac-address** *source-address* **continuous** [**interval** *milliseconds*] | **burst** [**interval** *milliseconds*][**number** *number*] [**frequency** *seconds*] [**size** *bytes*] **aggregation** *seconds* **duration** *seconds* | **max** *number-of-packets*

Cisco ASR 901 Routers
ip sla on-demand ethernetSLM *operation-number* | **domain** *domain-name* **evc** *evc-id* | **vlan** *vlan-id* **mpid** *target-mp-id* | **mac-address** *target-address* **cos** *cos* **source mpid** *source-mp-id* | **mac-address** *source-address* **continuous** [**interval** *milliseconds*] | **burst** [**interval** *milliseconds*][**number** *number*] [**frequency** *seconds*] [**size** *bytes*] **aggregation** *seconds* **duration** *seconds* | **max** *number-of-packets*

Syntax Description

DMMv1	Specifies that the frames sent are concurrent Ethernet frame Delay Measurement (ETH-DM) synthetic frames.
SLM	Specifies that the frames sent are Synthetic Loss Measurement (SLM) frames.
operation-number	Operation number of the already-configured IP SLAs operation to be referenced.
domain *domain-name*	Specifies the name of the Ethernet maintenance Operations, Administration & Maintenance (OAM) domain.
evc *evc-id*	Specifies the Ethernet Virtual Circuit (EVC) identification name.
vlan *vlan-id*	Specifies the VLAN identification number. The range is from 1 to 4096.
mpid *target-mp-id*	Specifies the identification numbers of the MEP at the destination. The range is from 1 to 8191.
mac-address *target-address*	Specifies the MAC address of the MEP at the destination.

cos *cos*	Specifies, for this MEP, which class of service (CoS) that will be sent in the Ethernet Connectivity Fault Management (CFM) message. The range is from 0 to 7.
source mpid *source-mp-id*	Specifies the identification numbers of the MEP being configured. The range is from 1 to 8191.
source mac-address *source-address*	Specifies the MAC address of the MEP being configured.
continuous	Specifies that a continuous stream of frames are to be sent during this on-demand operation.
burst	Specifies that burst of frames are to sent during this on-demand operation.
interval *milliseconds*	(Optional) Specifies the length of time in milliseconds (ms) between successive synthetic frames. The default is 1000 (1 second). The valid values are: • 10 • 20 • 25 • 50 • 100 • 1000
number *number-of-frames*	(Optional) Specifies the number of frames sent per burst. The value is 1 to 65535. The default is 10. **Note** The number per burst must be less than or equal to the value for **max**.

frequency *seconds*	(Optional) Specifies the number of seconds between bursts. The value is 1 to 900. The default is 60. **Note** The value for **frequency** must be greater than or equal to the value of *N*, where *N* is (**number**) X (**interval**) and greater than or equal to the value for **duration**.
size *bytes*	(Optional) Specifies payload size, in 4-octet increments, for the frames. The value is 64 to 384. The default is 64.
aggregation *seconds*	Specifies the length of time in seconds during which the performance measurements are conducted, after which the statistics are displayed. Value is 1 to 900. **Note** • The value for **aggregation** must be less than or equal to the value for**duration**. • For burst mode: The value for **aggregation** must be greater than and a multiple of the value for **frequency**.
duration *seconds*	Specifies the length of time in seconds, during which the on-demand operation runs. The value is 1 to 65535. **Note** • The value of **duration** must be greater than or equal to the value for **aggregation**. • For burst mode, the value for **duration** cannot be greater than the value for **frequency**.

max *number-of-packets*	Specifies the maximum number of packets sent during the on-demand operation. The value is 1 to 65535. **Note** • For burst mode, the value for **max** must be equal to or greater than the value for **number**. • For burst mode, the value for **duration** in max number of packets must be a multiple of the value for **size**.

Command Default

On-demand operations are not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(1)S	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to create and start a on-demand operation for generating statistics for Ethernet services. On-demand operations are pseudo operations that run in the background.

Use the *operation-number* argument with this command to create and run an on-demand operation in referenced mode. The operation being referenced must first be configured by using the **ethernet y1731 delay** and**ethernet y1731 loss** commands in IP SLA configuration mode.

Use the **domain** *domain-name* keyword and argument with the **ip sla on-demand ethernet** command to create and run an on-demand operation in direct mode.

For the burst mode of operation, the value of (number of frames) X (length of interval) must be less than or equal to the value of frequency, which must be less than or equal to the value of aggregation, which must be less than or equal to the value of duration.

To stop an on-demand operation, press **Ctrl-Shift-6**.

The **DMMv1** and **SLM** keywords for this command are not case sensitive. The keywords displayed in the online help contain uppercase letters to enhance readability only.

Examples

The following example shows how to configure an on-demand operation in reference mode for measuring frame loss. The operation to be referenced (11) must be configured before it can be referenced.

```
Device(config)# ip sla 11
Device(config-ip-sla)# ethernet y1731 loss SLM domain xxx vlan 10 mpid 3 cos 1 source mpid
 1
Device(config-sla-y1731-loss)# end
Device# ip sla on-demand ethernet slm 11 duration 38
```

The following example shows how to configure the same operation on-demand operation in direct mode:

```
Device# ip sla on-demand ethernet SLM domain xxx vlan 10 mpid 3 cos 1 source mpid 1 continuous
 aggregation 35 duration 38

Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  *20:17:41.535 PST Wed May 16 2012
 End time:  *20:18:16.535 PST Wed May 16 2012
 Number of measurements initiated: 35
 Number of measurements completed: 35
 Flag: OK

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Loss Statistics for Y1731 Operation 2984884426
Type of operation: Y1731 Loss Measurement
Latest operation start time: *20:17:41.535 PST Wed May 16 2012
Latest operation return code: OK
Distribution Statistics:


Interval 1
 Start time:  *20:17:41.535 PST Wed May 16 2012
 End time:  *20:18:16.535 PST Wed May 16 2012
 Number of measurements initiated: 35
 Number of measurements completed: 35
 Flag: OK

Forward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps forward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
Backward
  Number of Observations 3
  Available indicators: 0
  Unavailable indicators: 3
  Tx frame count: 30
  Rx frame count: 30
    Min/Avg/Max - (FLR % ): 0:9/000.00%/0:9
  Cumulative - (FLR % ): 000.00%
  Timestamps backward:
    Min - *20:18:10.586 PST Wed May 16 2012
    Max - *20:18:10.586 PST Wed May 16 2012
```

Related Commands

Command	Description
ethernet y1731 delay	Configures a sender Maintenance End Point (MEP) for an IP Service Level Agreements (SLAs) Metro Ethernet 3.0 (UTI-T Y.1731) delay or delay variation operation.
ethernet y1731 loss	Configures a sender Maintenance End Point (MEP) for an IP Service Level Agreements (SLAs) Metro Ethernet 3.0 (UTI-T Y.1731) frame loss operation.

ip sla periodic hostname resolution

To enable IP Service Level Agreements (SLAs) operation to use the recently resolved IPv4 or IPv6 destination address for probes specified with hostnames as destination, use the **ip sla periodic hostname resolution** command in global configuration mode. To return to the default value, use the **no** form of this command.

ip sla periodic hostname resolution
no ip sla periodic hostname resolution

Syntax Description

This command has no arguments or keywords.

Command Default

Periodic resolution of hostnames is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1	This command was introduced.

Usage Guidelines

This command is used to enable the periodic resolution of the hostnames specified in the IP SLA operations, such as, ICMP, ICMP-echo, UDP-echo, UDP-jitter and tcp-connect probes. By default, a hostname specified in the probe configuration is only resolved once during the configuration.

All hostnames are resolved every 120 seconds. If the time taken to resolve hostnames of all IP SLA operations is more than 120 seconds, the hostnames will be resolved after all the available hostnames are resolved.

Hostnames of IP SLA operations configured after enabling this command are resolved periodically. Hostnames of IP SLA operations configured earlier will not be resolved periodically.

If a hostname resolution fails, the corresponding operation will also fail.

For an IP SLA operation configured for specific VPN routing and forwarding (VRF), hostnames are resolved through the same VRF. Therefore, it is necessary to have VRF specific name servers.

Related Commands

Command	Description
show ip sla periodic hostname resolution	Displays the hostnames associated with IP Service Level Agreements (SLA) operations.

ip sla profile video

To specify a video profile name and enter a IP SLA VO profile endpoint configuration mode for configuring a user-defined video traffic profile for IP Service Level Agreements (SLAs) video operation, use the **ip sla profile video** command in global configuration mode. To remove the video profile, use the **no** form of this command.

ip sla profile video *profile-name*
no ip sla profile video *profile-name*

Syntax Description

profile-name	The following video profile names are valid options for the profile-name argument: • **CP-9900**: Cisco Unified 9900 Series IP Phone System (CP-9900) • **CTS**: Cisco Telepresence System 1000/3000 (CTS-1000/3000) • **custom**: Customized video endpoint type • *name*: User-defined unique identifier for profile.

Command Default

No video profile is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to specifiy a profile name and enter the IP SLA VO endpoint configuration mode for configuring a user-defined video traffic profile.

The keywords for this command are not case sensitive. The keywords in online help contain uppercase letters to enhance readability only.

Examples

```
Router(config)# ip sla video profile my-profile
Router(cfg-ipslavo-profile)# endpoint cts
Router(cfg-ipslavo-cts-profile)#
```

Related Commands

Command	Description
endpoint	Specifies endpoint type for a user-defined video profile.
show ip sla profile video	Displays a summary of IP SLAs video traffic profiles.

ip sla reaction-configuration

To configure proactive threshold monitoring parameters for an 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*]

Cisco ASR 901 Routers
ip sla reaction-configuration *operation-number* [**react unavailableDS** | **unavailableSD** | **loss-ratioDS** | **loss-ratioSD** [**threshold-type average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]] [**threshold-value** *upper-threshold lower-threshold*]]

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. • **jitterAvgPct**—Specifies that a reaction should occur if the percentile average round-trip jitter value violates the configured 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. • **jitterDSAvgPct** —Specifies that a reaction should occur if the percentile average one-way destination-to-source jitter value violates the configured 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. • **jitterSDAvgPCT** —Specifies that a reaction should occur if the percentile average one-way source-to-destination jitter value violates the configured 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. • **loss-ratioDS**—Specifies that a reaction should occur if the one-way destination-to-source loss-ratio violates the upper threshold or lower threshold. • **loss-ratioSD**—Specifies that a reaction should occur if the one way source-to-destination loss-ratio 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. • **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. • **rttPct** —Specifies that a reaction should occur if the percentile round-trip time violates the configured 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. • **unavailableDS**—Specifies that a reaction should occur if the percentage of destination-to-source Frame Loss Ratio (FLR) violates the upper threshold or lower threshold. • **unavailableSD**—Specifies that a reaction should occur if the percentage of source-to-destination FLR violates the upper threshold or lower threshold. • **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-typenever**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** —Transition one or more target operation's operational state from pending to active when the violation conditions are met. The target operations to be triggered are specified using the **ipslareaction-trigger** command.
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 **reactrttthreshold-typeaverage3** 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 **showipslareaction-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-valuey-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 (**xofy55**). The valid range for each value is from 1 to 16. The *x-value* will appear in the output of the **showipslareaction-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 the Default Threshold Values for Monitored Elements table in the “Usage Guidelines” section for a list of the default values. **Note** For MOS threshold values (**reactmos**), 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 **ipslamonitorreaction-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 **rtrreaction-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 **ipslamonitorreaction-configuration**command.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. This command replaces the **ipslamonitorreaction-configuration**command.
12.2(52)SE	This command was integrated into Cisco IOS Release 12.2(52)SE.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S. This command was modified. The **unavailableDS** and **unavailableSD** keywords for *monitored-element* argument were added for measuring Ethernet Frame Loss Ratio (FLR).

Release	Modification
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.3(2)T	This command was modified. The **jitterAvgPct**, **jitterDSAvgPct** , **jitterSDAvgPct** , **overThreshhold**, and **rttPct** keywords for the *monitored-element* argument to track the number of values above the threshold and determine the failure-to-success ratio of a percentile operation.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers. The **loss-ratioDS** and **loss-ratioSD** keywords were added.

Usage Guidelines

You can configure the **ipslareaction-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 **noipslareaction-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.

The **never** keyword option for the **threshold-type** keyword does not work with the **unavailableDS** and **unavailableSD** monitored elements for measuring Ethernet Frame Loss Ratio (FLR).

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 15.2(3)T, when an IP SLA operation is triggered, the (triggered) target operation starts and continues to run independently and without knowledge of the condition of the triggering operation. The target operation continues to run until its life expires, as specified by the lifetime configuration. The target operation must finish its life before it can be triggered again.

In Cisco IOS Release 15.2(3) and later releases, the (triggered) target operation runs until the condition-cleared event. Afetr which the target operation gracefully stops and the state of the target operation changes from Active to Pending so it can be triggered again.

Before Cisco IOS Release 15.1(1)T, valid online help was not available for this command. See the tables below 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 3: 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

monitored-element	**ICMP Echo**	**Path Echo**	**UDP Jitter**	**UDP Echo**	**TCP Connect**	**DHCP**	**DLSW**	**ICMP Jitter**	**DNS**	**Frame Relay**
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	—	—
latencySD	—	—	—	—	—	—	—	Y	—	—

monitored-element	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
packetLoss	—	—	—	—	—	—	—	Y	—	—

Table 4: 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						

Monitored Element	HTTP	SLM	RTP	FTP	LSP Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
iaJitterSD	—	—	Y	—	—	—	—	—	—
successivePacketLoss	—	—	—	—	—	—	—	—	—
maxOfLatencyDS	—	—	—	—	—	—	—	—	—
maxOfLatencySD	—	—	—	—	—	—	—	—	—
latencyDS	—	—	—	—	—	—	—	—	—
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 **noipslaresponder** 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.

The table below lists the action or combination of actions that are supported when a threshold event for a monitored element occurs.

Table 5: 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-serverenabletrapsrtr** or **snmp-serverenabletrapssyslog**command to enable the sending of IP SLAs SNMP trap notifications.

Use the **ipslaloggingtraps**command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications.

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 6: 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
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

Monitored Element Keyword	Upper Threshold	Lower Threshold
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 **showipslaconfiguration** command.

Note For ethernet Y1731 delay and loss measurement probes, if any changes are made to the reaction configuration for the supported react type variables while the probe is in active state or if the reaction configuration itself is removed for an active probe, then it is recommended to restart the probe for the configuration change to take effect.

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 **ipslareaction-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** globalconfiguration command).
target-operation	Number of the operation that will be triggered into an active state.

Command Default

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.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

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.

Command Default

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.

Command Default

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.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

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-ipaddresssource-hostname* [**client-id** *client-id*] [**group-name** *name*] [**endpoint-list** *template-name*] [**retry-timer** *minutes*]
no ip sla responder auto-register *source-ipaddresssource-hostname* [**client-id** *client-id*] [**endpoint-list** **template-name**] [**retry-timer** *minutes*]

Syntax Description

source-ipaddress	IP address of source for IP SLAs operation.
source-hostname	Hostname of source for IP SLAs operation.
client-id	(Optional) Specifies unique identifier for this responder.
client-id	(Optional) String of 1 to 64 alphanumeric characters.
group-name	(Optional) Specifies the group name.
name	(Optional) Group name to register.
endpoint-list	(Optional) Specifies unique identifier of auto IP SLAs endpoint list to which this responder will be added during autodiscovery.
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 autodiscovery 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 automeasure group.
discover (epl)	Enters IP SLA endpoint-list autodiscovery configuration mode for building an auto IP SLAs endpoint list using autodiscovery.
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.

Command Default

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 twamp

To enable an IP Service Letter Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) responder and configure the session-reflector function of the TWAMP responder, use the **ip sla responder twamp** command in global configuration mode. To disable the TWAMP responder, use the **no** form of this command.

ip sla responder twamp
no ip sla responder twamp

Syntax Description

This command has no keywords or arguments.

Command Default

An IP SLAs TWAMP responder is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command to configure a Cisco device as a session-reflector for an IP SLAs TWAMP responder and enter TWAMP reflector configuration mode.

For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector must be configured on the same device.

Examples

The following example shows how to configure a TWAMP session-reflector for an IP SLAs TWAMP responder:

```
Device(config)# ip sla responder twamp
Device(config-twamp-ref)# timeout 300
```

In the following example, the IP SLA TWAMP responder is disabled:

```
Router(config)# no ip sla responder twamp
Device(config)# exit
Device# show ip sla twamp session
IP SLAs Responder TWAMP is: Disabled
```

Related Commands

Command	Description
ip sla server twamp	Configures a device as a TWAMP server.
show ip sla twamp session	Displays TWAMP sessions.
timeout	Configures an inactivity timer for a TWAMP test session.

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.

Command Default

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* | **random** *milliseconds*] [**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.
random *milliseconds*	(Optional) Adds a random number of milliseconds (between 0 and the specified value) to the current time, after which the operation will start. The range is from 0 to 10000.
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.

Command Default

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.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.3(1)T	This command was modified. The **random** keyword was added for scheduling a random start time.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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.

Use the **random** keyword with the **start-time** keyword to randomly choose a scheduled start time for the operation. A random number of milliseconds between 0 and the specified value will be added to the current time to define the start time. The value provided for the random start time applies only to the first time the operation runs after which normal frequency rules apply.

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.

Command	Description
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.

ip sla server twamp

To configure the server function of an IP Service Letter Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) responder and enter TWAMP server configuration mode, use the **ip sla server twamp** command in global configuration mode. To disable the TWAMP server, use the **no** form of this command.

ip sla server twamp
no ip sla server twamp

Syntax Description

This command has no keywords or arguments.

Command Default

The TWAMP server function of an IP SLAs TWAMP responder is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command to configure a Cisco device as a TWAMP server for an IP SLAs TWAMP responder and enter the TWAMP server configuration mode.

For IP SLAs TWAMP Responder v1.0, the TWAMP server and the session-reflector must be configured on the same device.

Examples

The following example shows how to configure a TWAMP server:

```
Device(config)# ip sla server twamp
Device(config-twamp-srvr)# port 9000
Device(config-twamp-srvr)# timer inactivity 300
```

Related Commands

Command	Description
ip sla responder twamp	Enables a TWAMP responder.
port (twamp)	Configures a port for listening.
timer inactivity	Configures an inactivity timer for a TWAMP control session.

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.

Command Default

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 monitor configuration mode. To remove the definition, use the no form of this command.

lsr-path host *name1ip-address1* [[*hostname2ip-address2*]. . . [*hostname8ip-address8*]]
no lsr-path

Syntax Description

host name1 | 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.

Command Default

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)

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 the table below). 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 the table below) 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 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

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 the table above).

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.

max-delay

To configure the maximum length of time a Maintenance Endpoint (MEP) in an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation waits for a synthetic frame, use the **max-delay** command in IP SLA Y1731 delay configuration mode. To return to the default, use the **no** form of this command.

max-delay *milliseconds*
no **max-delay**

Syntax Description

milliseconds	Maximum delay in milliseconds (ms). The range is from 1 to 65535. The default is 5000.

Command Default

The default for max-delay is 5000 milliseconds.

Command Modes

IP SLA Y.1731 delay configuration (config-sla-y1731-delay)

Command History

Release	Modification
15.1(2)S	This command was introduced.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to change the maximum amount of time an MEP in an Ethernet delay or delay variation operation will wait for a synthetic frame from the default (5000 ms) to the specified value.

Examples

```
Router(config-term)# ip sla 501
Router(config-ip-sla)# ethernet y1731 delay receive 1DM domain xxx evc yyy cos 3 mpid 101
Router(config-sla-y1731-delay)# max-delay 2000
```

```
Router# show ip sla configuration 501

IP SLAs Infrastructure Engine-III
Entry number: 501
Owner: admin
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: xxx
ReceiveOnly: TRUE
Evc: yyy
Local Mpid: 101
CoS: 3
   Max Delay: 5000
Threshold (milliseconds): 2000
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

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.

measurement-type

To configure parameters for the measurement metrics to be collected by an IP Service Level Agreements (SLAs) service performance operation, use the **measurement-type** command in IP SLA service performance configuration mode. To return to default, use the **no** form of this command.

measurement-type direction external | internal
no measurement-type direction

Syntax Description

external	Specifies the direction of the measurement.
internal	Specifies the direction of the measurement. This is the default.

Command Default

The measurement type is internal.

Command Modes

IP SLA service performance configuration (config-ip-sla-service-performance)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

Throughput testing can be unidirectional or bidirectional, with independent throughput tests in each direction. This command with the **direction** keyword configures the directions for which the testing is performed.

Use the **show ip sla configuration** command to display configuration command to display configuration values, including all defaults, for all Cisco IOS IP SLAs operations or for a specified operation.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
VLAN:
Interface: GigabitEthernet0/4
Service Instance: 10
EVC Name:
Duration Time: 20
Interval Buckets: 5

Signature:
05060708

Description: this is with all operation modes

Measurement Type:
throughput, loss
Direction: internal

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
```

```
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
Schedule:
   Operation frequency (seconds): 64  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
```

Related Commands

Command	Description
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

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.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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

Multicast UDP jitter configuration (config-ip-sla-multicast-jitter-oper)

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.
15.2(4)M	This command was modified. The multicast UDP jitter configuration mode was added.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

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.

optimize timestamp

To optimize the time stamp location for more accurate RTT measurements during IP Service Level Agreements (SLAs) UDP jitter operations, use the **optimize timestamp** command in UDP jitter configuration mode. To return to the default value, use the **no** form of this command.

optimize timestamp
no optimize timestamp

Syntax Description

This command has no arguments or keywords.

Command Default

Time stamp location is not optimized

Command Modes

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

Command History

Release	Modification
Cisco IOS XE 3.7S	This command was introduced. This command is supported on the Cisco ASR 1000 Series Aggregation Services router only.

Usage Guidelines

This command optimizes the time-stamp location for IP SLAs for more accurate RTT measurements when QFP time stamping is enabled for an IP SLAs UDP jitter operation.

If you configure this command on a source device, the responder must also support the optimized time stamp location or the IP SLAs operation will fail.

Before configuring the **optimize time stamp** command, you must first configure the **precision microseconds** command to enable QFP time stamping. The devices on which the UDP probe and IP SLAs responder are configured must both be running Cisco software images that support QFP time stamping in order for the QFP Time Stamping feature to work.

You must configure the type of IP SLAs operation (such as UDP 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.

IP SLAs UDP jitter operations support both IPv4 and IPv6 operations.

Examples

```
IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 192.0.2.25/0.0.0.0
Target port/Source port: 8989/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 64
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Operation Stats Precision : microseconds !<=enables QFP time stamping
Timestamp Location Optimization: Enabled !<=optimizes time stamp location
Operation Packet Priority : normal
NTP Sync Tolerance : 0 percent
```

```
Vrf Name:
Control Packets: enabled
Schedule:
 Operation frequency (seconds): 60 (not considered if randomly scheduled)
 Next Scheduled Start Time: Start Time already passed
 Group Scheduled : FALSE
 Randomly Scheduled : FALSE
 Life (seconds): 3600
 Entry Ageout (seconds): never
 Recurring (Starting Everyday): FALSE
 Status of entry (SNMP RowStatus): Active
 Threshold (milliseconds): 5000
Distribution Statistics:
 Number of statistic hours kept: 2
 Number of statistic distribution buckets kept: 1
 Statistic distribution interval (microseconds): 20
 Enhanced History:
```

Related Commands

Command	Description
no ip sla	Removes the configuration for an IP SLAs operation.
precision microseconds	Enables QFP time stamping.
show ip sla configuration	Displays configuration values, including all defaults, for all IP SLAs operations or for a specified operation.

outer-cos

To set the class of service (CoS) for the outer loop in a service performance packet profile, use the **outer-cos** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

outer-cos *cos-number*
no outer-cos

Syntax Description

cos-number	Class of service (CoS) value. The range is from 0 to 7.

Command Default

No CoS number for the outer loop is configured in the packet profile.

Command Modes

Packet profile submode of IP SLA service performance configuration (config-ip-sla-service-packet)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
.
.
.

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
.
.
.
```

Related Commands

Command	Description
profile packet	Creates a packet profile for live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

outer-eth-type

To set the encapsulation type that will be populated in the outer VLAN tag of the packet, use the **outer-eth-type** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

outer-eth-type { dot1ad | dot1q }

Command Default

If you do not specify encapsulation type in the packet profile, it is considered as dot1q encapsulation.

Command Modes

Packet profile submode of IP SLA service performance configuration (config-ip-sla-service-performance-packet)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 0010.0010.0010
.
.
.

Profile Traffic:
Direction: internal
CIR: 10000
EIR: 20000
CBS: 0
EBS: 0
Burst Size: 0
Burst Duration: 0
Inter Burst Interval: 0
Rate Step (kbps): 30000
Mode: conform-color
Action: Transmit
Set COS: 2
Mode: exceed-color
Action: Transmit
Set COS: 7
Mode:
Action: Transmit
Set COS: 0
Set Tunnel EXP: 0

Profile Packet[0] :
Inner COS: Not Set
Outer COS: 3
Inner VLAN: Not Set
Outer VLAN: 100
DSCP: default
```

```
Packet Size: 1024
Source MAC Address: 0020.0020.0020
EtherType: default
outer-eth-type: dot1q
inner-eth-type: dot1q

Number of Packets: 100
.
.
.
```

Related Commands

Command	Description
inner-eth-type	Sets the encapsulation type for the inner VLAN tag.

outer-vlan

To specify a VLAN for the outer loop in a service performance packet profile, use the **outer-vlan** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

outer-vlan *vlan-id*
no outer-vlan *vlan-id*

Syntax Description

vlan-id	VLAN identifier. The range is from 0 to 4096.

Command Default

No VLAN for the outer loop is configured in the packet profile.

Command Modes

Packet profile submode of IP SLA service performance configuration (config-ip-sla-service-packet)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
.
.
.

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
.
.
.
```

Related Commands

Command	Description
profile packet	Creates a packet profile for live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

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, IP SLA monitor configuration, or IP SLA Y.1737 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. Value is from 0 to 255 ASCII characters.

Command Default

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)

Multicast UDP jitter configuration (config-ip-sla-multicast-jitter-oper)

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)

Video (config-ip-sla-video)

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)

IP SLA Y.1731 Configuration

Delay configuration (config-sla-y1731-delay)

Loss configuration (config-sla-y1731-loss)

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.

Release	Modification
12.2(33)SXI	The Ethernet echo, Ethernet jitter, and Ethernet parameters configuration modes were added.
12.2(58)SE	This command was modified. Support for the video configuration submode of IP SLA configuration mode was added.
15.1(2)S	This command was modified. Support for the IP SLA Y.1731 configuration mode was added.
15.2(2)T	This command with support for the video configuration submode of IP SLA configuration mode was integrated into Cisco IOS Release 15.2(2)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.2(4)M	This command was modified. The multicast UDP jitter configuration mode was added.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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 the table below). 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 the table below) and the operation type configured.

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 , 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

Examples

The following examples show how to set the owner of an IP SLAs ICMP echo operation to 172.16.1.189 cwb.cisco.com User1 RTP 555-0100.

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:

```
Router# show ip sla configuration 1

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:

```
Router# show ip sla configuration 1

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
```

IP SLA Y.1737 Configuration

This example shows the **owner** command being used in the configuration for an IP SLAs Metro 3.0 (ITU-T Y.1731) delay operation:

```
Router# show ip sla configuration 10

IP SLAs Infrastructure Engine-III
Entry number: 10
Owner: 172.16.1.189 cwb.cisco.com User1 RTP 555-0100
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
```

```
Frame Type: DMM
Domain: xxx
Vlan: yyy
Target Mpid: 101
Source Mpid: 100
CoS: 4
   Max Delay: 5000
   Request size (Padding portion): 64
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
.
.
.
```

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.

packet-size

To specify a size for packets in a service performance packet profile, use the **packet-size** command in the packet profile submode of IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

packet-size *size*
no packet-size *size*

Syntax Description

size	Size of a packet in bytes. The following keywords are valid for this argument: • **64**—This is the default. • **128** • **256** • **512** • **1280** • **1518**

Command Default

The packet size in the packet profile is 64 bytes.

Command Modes

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

You must configure a packet profile before you can configure parameters for the profile.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
.
.
.

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
```

```
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
.
.
.
```

Related Commands

Command	Description
profile packet	Creates a packet profile for live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

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-addressdestination-hostname* [**source-ip** *ip-addresshostname*]

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.

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. 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.
15.2(3)T	This command was modified. Support for IPv6 addresses was added.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

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
```

In the following example, IP SLAs operation 1 is configured as an ICMP path echo operation in Cisco IOS Release 15.2(3)T using the IP/ICMP protocol and an IPv6 destination address:

```
ip sla 1
 path-echo 2001:10:10:10::3
!
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-addressdestination-hostname* [**source-ip** *ip-addresshostname*] [**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).

Command Default

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.
15.2(3)T	This command was modified. Support for IPv6 addresses was added.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

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
```

The following example show how to enable the ICMP path jitter operation in an IPv6 network to trace the IP path to the destination 2001:10:10:10::3 and send 50 test packets to each hop with an interval of 30 ms between each test packe. IPv6 addresses are supported in Cisco IOS Release 15.2(3)T and later releases.

```
ip sla 20
 path-jitter 2001:10:10:10::3 num-packets 50 interval 30
!
ip sla schedule 20 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.

Command Default

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)

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 the table below). 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 the table below) 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 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

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 the table above).

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.

percentile

To configure percentile support for filtering outliers for Cisco IP Service Level Agreements (SLAs) operations, use the **percentile** command in Ethernet jitter, ICMP jitter, or UDP jitter configuration mode. To remove the percentile configuration, use the **no** form of this command.

percentile jitteravg | **jitterds** | **jittersd** | **owds** | **owsd** | **rtt** *percent*
no percentile jitteravg | **jitterds** | **jittersd** | **owds** | **owsd** | **rtt**

Syntax Description

jitteravg	Specifies that average jitter packets be filtered.
jitterds	Specifies that one-way destination-to-source interarrival jitter packets be filtered.
jittersd	Specifies that one-way source-to-destination interarrival jitter packets be filtered.
owds	Specifies that one-way destination-to-source packets be filtered.
owsd	Specifies that fone-way source-to-destination packets be filtered.
rtt	Specifies that round-trip-time (RTT) packets be filtered.
percent	Percentage (%) of packets to be used for calculations. The range is from 90 to 100. The default is 100.

Command Default

All packets will be processed.

Command Modes

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

ICMP jitter configuration (config-ip-sla-icmpjitter)

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

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use this command to configure an IP SLAs operation to measure values that are within a specified percentile, such as the 95 percentile of RTT, in order to examine a set of measurements that are 95% faster than and 5% slower than the rest of the data.

To track the number of values above a specified threshold and determine the failure-to-success ratio, use the **ip sla reaction-configuration** command in global configuration mode.

To display the percentile statistics when an operation is configured with the percentile option, use the **show ip sla statistics** command.

Example

The following example shows how to configure an IP SLAs ICMP jitter operation with the percentile option:

```
ip sla 1
 icmp-jitter 192.168.0.129 interval 40 num-packets 100 source-ip 10.1.2.34
 percentile jitteravg 95
!
ip sla reaction-configuration 1 react jitterAvgpct 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 reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or for an individual operation.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or for a n individual operation.

port (twamp)

To specify the port to be used by the server function of an IP Service Level Agreements (SLAs) Two-Way Active Measurement Protocol (TWAMP) responder, use the **port** command in TWAMP server configuration mode. To remove the port configuration, use the **no** form of this command.

port *port-number*
no port

Syntax Description

port-number	Number of port. The range is from 1 to 65353. The default is device specific.

Command Default

A device-specific default port is use by the TWAMP server.

Command Modes

TWAMP server configuration (config-twamp-srvr)

Command History

Release	Modification
15.2(2)S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command to specifiy the port to be used by the TWAMP server to listen for connection and control requests. The same port negotiates for the port to which performance probes are sent. The configured port must not be an IANA well-known port or any port that is used by other applications.

Examples

The following example shows how to configure a TWAMP server:

```
Device(config)# ip sla server twamp
Device(config-twamp-srvr)# port 9000
Device(config-twamp-srvr)# timer inactivity 300
```

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). In Cisco IOS XE Release 3.7S and later releases: E nables IP SLAs QFP Time Stamping.

Command Default

Milliseconds precision is configured.

Command Modes

IP SLA Configuration

Multicast UDP jitter configuration (config-ip-sla-multicast-jitter-oper)

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.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S. This command with the **microseconds** keyword enables IP SLAs QFP Time Stamping.
15.2(4)M	This command was modified. The multicast UDP jitter configuration mode was added.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Release	Modification
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.

Usage Guidelines

If the **milliseconds** keyword is configured, 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.

In Cisco IOS XE 3.7S and later releases, configure the **precision microseconds** command to enable IP SLAs QFP Time Stamping.

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

Note The **precisionmicroseconds** command requires that both the source and IP SLAs Responder devices are running a version of Cisco IOS software that supports the **precisionmicroseconds** command. See the “Command History” table for information about the supported Cisco IOS software releases.

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 the table below). 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 the table below) 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 10: Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T, 12.0(32)SY, 12.2(33)SRB, 12.2(33)SB, Cisco IOS XE 3.7S, and 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 the table above).

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
```

The following sample configuration shows how to enable QFP time stamping and to optimize the time stamp location for more accurate RTT measurements.

```
ip sla 1
 udp-jitter 192.0.2.134 5000 num-packets 20
 request-data-size 160
 tos 128
 frequency 30
 precision microseconds
 optimize timestamp
!
ip sla schedule 1 start-time after 00:05:00
```

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.
optimize timestamp	Optimizes the time stamp location.

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-packetpriority** command is replaced by the operation-packet-priority command. See the **operation-packetpriority** command for more information.

To specify the packet priority of a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **probe-packetpriority**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)

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-packetprority** 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 the table below). 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-packetpriority** command varies depending on the Cisco IOS release you are running (see the table below) 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-packetpriority** command in UDP jitter configuration mode (config-sla-monitor-jitter) within IP SLA monitor configuration mode.

Table 11: 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 he table above).

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.

profile packet

To begin configuring a packet profile for an IP Service Level Agreements (SLAs) service performance operation and enter the packet profile submode of IP SLA service performance configuration mode, use the **profile packet** command in IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

profile packet
no profile packet

This command has no argument or keywords

Command Default

No packet profile is configured.

Command Modes

IP SLA service performance configuration (config-ip-sla-service-performance)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

Use this command to define the packets to be sent in the live traffic for an IP SLAs service performance operation.

Before configuring a packet profile, you must use the **profile traffic** command to configure a traffic profile for generating live traffic.

Use the **show ip sla configuration** command to display configuration command to display configuration values, including all defaults, for all Cisco IOS IP SLAs operations or for a specified operation.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
VLAN:
Interface: GigabitEthernet0/4
Service Instance: 10
EVC Name:
Duration Time: 20
Interval Buckets: 5

Signature:
05060708

Description: this is with all operation modes

Measurement Type:
throughput, loss
Direction: internal

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
```

```
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
Schedule:
   Operation frequency (seconds): 64  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
```

Related Commands

Command	Description
profile traffic	Configures a traffic profile for generating live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

profile traffic

To begin configuring a traffic profile for an IP Service Level Agreements (SLAs) service performance operation and enter the traffic profile submode of IP SLA service performance configuration mode, use the **profile traffic** command in IP SLA service performance configuration mode. To return to the default, use the **no** form of this command.

profile traffic directionexternal | internal
no profile traffic direction

Syntax Description

direction	Specifies the direction for the generated traffic.
external	Direction of the traffic.
internal	Direction of the traffic.

Command Default

No traffic profile is configured and no live traffic is generated.

Command Modes

IP SLA service performance

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

Use this command to configure an inline traffic profile for generating live traffic for an IP SLAs service performance operation. A traffic profile defines an upper bound on the volume of the expected service frames belonging to a particular service instance.

Do *not* configure a traffic profile for collecting measurements in passive measurement mode.

Use the **show ip sla configuration** command to display configuration command to display configuration values, including all defaults, for all Cisco IOS IP SLAs operations or for a specified operation.

```
IP SLAs Infrastructure Engine-III
Entry number: 1
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
VLAN:
Interface: GigabitEthernet0/4
Service Instance: 10
EVC Name:
Duration Time: 20
Interval Buckets: 5

Signature:
05060708

Description: this is with all operation modes

Measurement Type:
throughput, loss
```

```
Direction: internal

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 3
Burst Interval: 20
Rate Step (kbps): 1000 2000

Profile Packet:
Inner COS: 6
Outer COS: 6
Inner VLAN: 100
Outer VLAN: 100
Source MAC Address: 4055.398d.8d4c
Packet Size: 512
Schedule:
   Operation frequency (seconds): 64  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
```

Related Commands

Command	Description
profile packet	Configures a packet profile for live traffic.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.