



## CHAPTER 42

# Configuring Cisco IOS IP SLAs Operations

---

## Finding Feature Information

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Prerequisites for Configuring Cisco IOS IP SLAs Operations

- Before configuring any IP SLAs application, we recommend that you verify the operation type supported on your software image by using the **show ip sla application** privileged EXEC command.

## Restrictions for Configuring Cisco IOS IP SLAs Operations

- The IP SLAs responder can be a Cisco IOS Layer 2, responder-configurable switch, such as a Catalyst 2960 or IE 2000 switch running the LAN Base image, or a Catalyst 3560 or 3750 switch running the IP base image. The responder does not need to support full IP SLAs functionality.
- The switch does not support Voice over IP (VoIP) service levels using the gatekeeper registration delay operations measurements. Before configuring any IP SLAs application, you can use the **show ip sla application** privileged EXEC command to verify that the operation type is supported on your software image.

## Information About Configuring Cisco IOS IP SLAs Operations

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the switch. Cisco IP SLAs is a part of Cisco IOS software that allows Cisco customers to analyze IP service levels for IP applications and services by using active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. With Cisco IOS IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting.

## Cisco IOS IP SLAs

Cisco IOS IP SLAs sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services and collects network performance information in real time. Cisco IOS IP SLAs generates and analyzes traffic either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurements provided by the various Cisco IOS IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Depending on the specific Cisco IOS IP SLAs operation, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLAs packets have configurable IP and application layer options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs is Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs collects a unique subset of these performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time

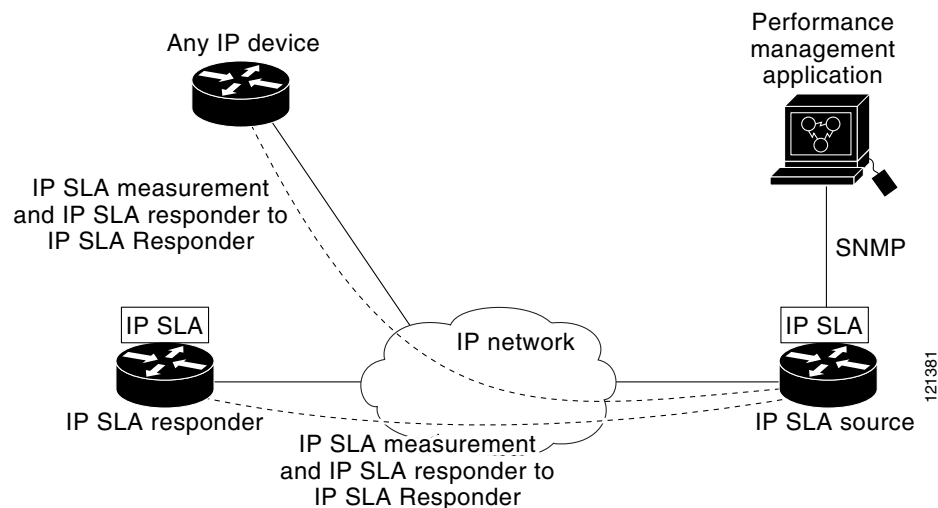
Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like CiscoWorks Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products. Using IP SLAs can provide these benefits:

- Service-level agreement monitoring, measurement, and verification.
- Network performance monitoring
  - Measures the jitter, latency, or packet loss in the network.
  - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment to verify that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).
- Troubleshooting of network operation by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the switch supports MPLS)

## Cisco IOS IP SLAs to Measure Network Performance

You can use IP SLAs to monitor the performance between any area in the network—core, distribution, and edge—without deploying a physical probe. It uses generated traffic to measure network performance between two networking devices. Figure 42-1 shows how IP SLAs begins when the source device sends a generated packet to the destination device. After the destination device receives the packet, depending on the type of IP SLAs operation, it responds with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.

**Figure 42-1** Cisco IOS IP SLAs Operation



To implement IP SLAs network performance measurement, you need to perform these tasks:

1. Enable the IP SLAs responder, if required.
2. Configure the required IP SLAs operation type.
3. Configure any options available for the specified operation type.
4. Configure threshold conditions, if required.
5. Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using the Cisco IOS CLI or a network management system (NMS) system with SNMP.

## IP SLAs Responder and IP SLAs Control Protocol

The IP SLAs responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without the need for dedicated probes. The responder uses the Cisco IOS IP SLAs Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond. Only a Cisco IOS device can be a source for a destination IP SLAs Responder.

Figure 42-1 shows where the Cisco IOS IP SLAs responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLAs operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time,

the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLAs packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

You do not need to enable the responder on the destination device for all IP SLAs operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP). You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.

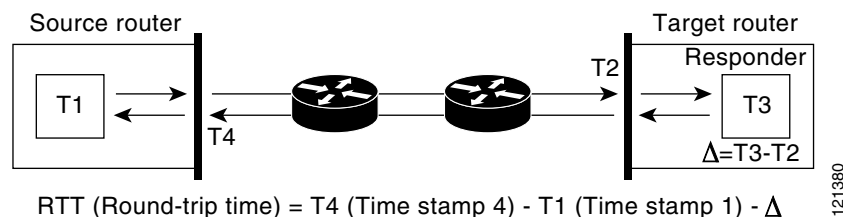
## Response Time Computation for IP SLAs

Switches and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays.

When the IP SLAs responder is enabled, it allows the target device to take time stamps when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-milliseconds (ms).

Figure 42-2 demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled, time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.

**Figure 42-2 Cisco IOS IP SLAs Responder Time Stamping**



An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements, you must configure both the source router and target router with Network Time Protocol (NTP) so that the source and target are synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

## IP SLAs Operation Scheduling

When you configure an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the pending option to set the operation to start at a later time.

The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations on a switch running the IP services image by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLAs operations helps minimize the CPU utilization and thus improves network scalability.

## IP SLAs Operation Threshold Monitoring

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as these:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency

An IP SLAs threshold violation can also trigger another IP SLAs operation for further analysis. For example, the frequency could be increased or an ICMP path echo or ICMP path jitter operation could be initiated for troubleshooting.

Determining the type of threshold and the level to set can be complex, and depends on the type of IP service being used in the network.

## IP Service Levels by Using the UDP Jitter Operation

Jitter means interpacket delay variance. When multiple packets are sent consecutively 10 ms apart from source to destination, if the network is behaving correctly, the destination should receive them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be more than or less than 10 ms with a positive jitter value meaning that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, positive jitter is 2 ms; if the packets arrive 8 ms apart, negative jitter is 2 ms. For delay-sensitive networks, positive jitter values are undesirable, and a jitter value of 0 is ideal.

In addition to monitoring jitter, the IP SLAs UDP jitter operation can be used as a multipurpose data gathering operation. The packets IP SLAs generates carry packet sending and receiving sequence information and sending and receiving time stamps from the source and the operational target. Based on these, UDP jitter operations measure this data:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)

- Round-trip delay (average round-trip time)

Because the paths for the sending and receiving of data can be different (asymmetric), you can use the per-direction data to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation generates synthetic (simulated) UDP traffic and sends a number of UDP packets, each of a specified size, sent a specified number of milliseconds apart, from a source router to a target router, at a given frequency. By default, ten packet-frames, each with a payload size of 10 bytes are generated every 10 ms, and the operation is repeated every 60 seconds. You can configure each of these parameters to best simulate the IP service you want to provide.

To provide accurate one-way delay (latency) measurements, time synchronization, such as that provided by NTP, is required between the source and the target device. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data is returned, but values of 0 are returned for the one-way delay measurements provided by the UDP jitter operation

**Note**

---

Before you configure a UDP jitter operation on the source device, you must enable the IP SLAs responder on the target device (the operational target).

---

## IP Service Levels by Using the ICMP Echo Operation

The ICMP echo operation measures end-to-end response time between a Cisco device and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements between the source IP SLAs device and the destination IP device. The IP SLAs ICMP echo operation conforms to the same specifications as ICMP ping testing, and the two methods result in the same response times.

**Note**

---

This operation does not require the IP SLAs responder to be enabled.

---

## How to Configure Cisco IOS IP SLAs Operations

**Note**

---

Not all of the IP SLAs commands or operations described in this guide are supported on the switch. The switch supports IP service level analysis by using UDP jitter, UDP echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, FTP, DNS, and DHCP, as well as multiple operation scheduling and proactive threshold monitoring. It does not support VoIP service levels using the gatekeeper registration delay operations measurements.

---

## Configuring the IP SLAs Responder

### Before You Begin

For the IP SLAs responder to function, you must also configure a source device, such as a Catalyst 3750 or Catalyst 3560 switch running the IP services image, that has full IP SLAs support. Refer to the documentation for the source device for configuration information.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>ip sla responder {tcp-connect   udp-echo} ipaddress ip-address port port-number</code>	Configures the switch as an IP SLAs responder. The optional keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>tcp-connect</b>—Enables the responder for TCP connect operations.</li> <li>• <b>udp-echo</b>—Enables the responder for User Datagram Protocol (UDP) echo or jitter operations.</li> <li>• <b>ipaddress ip-address</b>—Enters the destination IP address.</li> <li>• <b>port port-number</b>—Enters the destination port number.</li> </ul> <b>Note</b> The IP address and port number must match those configured on the source device for the IP SLAs operation.
Step 3	<code>end</code>	Returns to privileged EXEC mode.

## Configuring UDP Jitter Operation

### Before You Begin

Before you configure a UDP jitter operation on the source device, you must enable the IP SLAs responder on the target device (the operational target).

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>ip sla operation-number</code>	Creates an IP SLAs operation, and enters IP SLAs configuration mode.

	Command	Purpose
Step 3	<b>udp-jitter</b> { <i>destination-ip-address</i>   <i>destination-hostname</i> } <i>destination-port</i> [ <b>source-ip</b> { <i>ip-address</i>   <i>hostname</i> }] [ <b>source-port</b> <i>port-number</i> ] [ <b>control</b> { <b>enable</b>   <b>disable</b> }] [ <b>num-packets</b> <i>number-of-packets</i> ] [ <b>interval</b> <i>interpacket-interval</i> ]	Configures the IP SLAs operation as a UDP jitter operation, and enters UDP jitter configuration mode. <ul style="list-style-type: none"> <li>• <i>destination-ip-address</i>   <i>destination-hostname</i>—Specifies the destination IP address or hostname.</li> <li>• <i>destination-port</i>—Specifies the destination port number in the range from 1 to 65535.</li> <li>• (Optional) <b>source-ip</b> {<i>ip-address</i>   <i>hostname</i>}—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.</li> <li>• (Optional) <b>source-port</b> <i>port-number</i>—Specifies the source port number in the range from 1 to 65535. When a port number is not specified, IP SLAs chooses an available port.</li> <li>• (Optional) <b>control</b>—Enables or disables sending of IP SLAs control messages to the IP SLAs responder. By default, IP SLAs control messages are sent to the destination device to establish a connection with the IP SLAs responder.</li> <li>• (Optional) <b>num-packets</b> <i>number-of-packets</i>—Enters the number of packets to be generated. The range is 1 to 6000; the default is 10.</li> <li>• (Optional) <b>interval</b> <i>inter-packet-interval</i>—Enters the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms.</li> </ul>
Step 4	<b>frequency</b> <i>seconds</i>	(Optional) Sets the rate at which a specified IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
Step 5	<b>exit</b>	Exits UDP jitter configuration mode, and returns to global configuration mode.



	Command	Purpose
Step 6	<b>ip sla schedule</b> <i>operation-number</i> [ <b>life</b> { <b>forever</b>   <i>seconds</i> }] [ <b>start-time</b> { <i>hh:mm</i> [: <i>ss</i> ] [ <i>month day</i>   <i>day month</i> ]}   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i> ] [ <b>ageout</b> <i>seconds</i> ] [ <b>recurring</b> ]	Configures the scheduling parameters for an individual IP SLAs operation. <ul style="list-style-type: none"> <li>• <i>operation-number</i>—Enters the RTR entry number.</li> <li>• (Optional) <b>life</b>—Sets the operation to run indefinitely (<b>forever</b>) or for a specific number of <i>seconds</i>. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).</li> <li>• (Optional) <b>start-time</b>—Enters the time for the operation to begin collecting information: <ul style="list-style-type: none"> <li>– To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.</li> <li>– Enter <b>pending</b> to select no information collection until a start time is selected.</li> <li>– Enter <b>now</b> to start the operation immediately.</li> <li>– Enter <b>after</b> <i>hh:mm:ss</i> to show that the operation should start after the entered time has elapsed.</li> </ul> </li> <li>• (Optional) <b>ageout</b> <i>seconds</i>—Enters the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out).</li> <li>• (Optional) <b>recurring</b>—Sets the operation to automatically run every day.</li> </ul>
Step 7	<b>end</b>	Returns to privileged EXEC mode.

## Analyzing IP Service Levels by Using the ICMP Echo Operation



### Note

This operation does not require the IP SLAs responder to be enabled.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enters global configuration mode.
Step 2	<b>ip sla</b> <i>operation-number</i>	Creates an IP SLAs operation and enters IP SLAs configuration mode.
Step 3	<b>icmp-echo</b> { <i>destination-ip-address</i>   <i>destination-hostname</i> } [ <b>source-ip</b> { <i>ip-address</i>   <i>hostname</i> }   <b>source-interface</b> <i>interface-id</i> ]	Configures the IP SLAs operation as an ICMP Echo operation and enters ICMP echo configuration mode. <ul style="list-style-type: none"> <li>• <i>destination-ip-address</i>   <i>destination-hostname</i>—Specifies the destination IP address or hostname.</li> <li>• (Optional) <b>source-ip</b> {<i>ip-address</i>   <i>hostname</i>}—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.</li> <li>• (Optional) <b>source-interface</b> <i>interface-id</i>—Specifies the source interface for the operation.</li> </ul>
Step 4	<b>frequency</b> <i>seconds</i>	(Optional) Sets the rate at which a specified IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.

	Command	Purpose
Step 5	<b>exit</b>	Exits UDP jitter configuration mode, and returns to global configuration mode.
Step 6	<b>ip sla schedule</b> <i>operation-number</i> [ <b>life</b> { <b>forever</b>   <i>seconds</i> }] [ <b>start-time</b> { <i>hh:mm [:ss]</i> [ <i>month</i> <i>day</i>   <i>day month</i> ]   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i> ] [ <b>ageout</b> <i>seconds</i> ] [ <b>recurring</b> ]	Configures the scheduling parameters for an individual IP SLAs operation. <ul style="list-style-type: none"> <li><i>operation-number</i>—Enters the RTR entry number.</li> <li>(Optional) <b>life</b>—Sets the operation to run indefinitely (<b>forever</b>) or for a specific number of <i>seconds</i>. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).</li> <li>(Optional) <b>start-time</b>—Enters the time for the operation to begin collecting information: <ul style="list-style-type: none"> <li>To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.</li> <li>Enter <b>pending</b> to select no information collection until a start time is selected.</li> <li>Enter <b>now</b> to start the operation immediately.</li> <li>Enter <b>after</b> <i>hh:mm:ss</i> to indicate that the operation should start after the entered time has elapsed.</li> </ul> </li> <li>(Optional) <b>ageout</b> <i>seconds</i>—Enters the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds; the default is 0 seconds (never ages out).</li> <li>(Optional) <b>recurring</b>—Sets the operation to automatically run every day.</li> </ul>
Step 7	<b>end</b>	Returns to privileged EXEC mode.

## Monitoring and Maintaining Cisco IP SLAs Operations

Command	Purpose
<b>show ip sla application</b>	Displays global information about Cisco IOS IP SLAs.
<b>show ip sla authentication</b>	Displays IP SLAs authentication information.
<b>show ip sla configuration</b> [ <i>entry-number</i> ]	Displays configuration values including all defaults for all IP SLAs operations or a specific operation.
<b>show ip sla enhanced-history</b> { <b>collection-statistics</b>   <b>distribution statistics</b> } [ <i>entry-number</i> ]	Displays enhanced history statistics for collected history buckets or distribution statistics for all IP SLAs operations or a specific operation.
<b>show ip sla ethernet-monitor configuration</b> [ <i>entry-number</i> ]	Displays IP SLAs automatic Ethernet configuration.
<b>show ip sla event-publisher</b>	Displays the list of client applications that are registered to receive IP SLAs notifications.
<b>show ip sla group schedule</b> [ <i>schedule-entry-number</i> ]	Displays IP SLAs group scheduling configuration and details.
<b>show ip sla history</b> [ <i>entry-number</i>   <b>full</b>   <b>tabular</b> ]	Displays history collected for all IP SLAs operations

Command	Purpose
<b>show ip sla mpls-lsp-monitor</b> { <b>collection-statistics</b>   <b>configuration</b>   <b>ldp</b> <b>operational-state</b>   <b>scan-queue</b>   <b>summary</b> [ <i>entry-number</i> ]   <b>neighbors</b> }	Displays MPLS label switched path (LSP) Health Monitor operations.
<b>show ip sla reaction-configuration</b> [ <i>entry-number</i> ]	Displays the configured proactive threshold monitoring settings for all IP SLAs operations or a specific operation.
<b>show ip sla reaction-trigger</b> [ <i>entry-number</i> ]	Displays the reaction trigger information for all IP SLAs operations or a specific operation.
<b>show ip sla responder</b>	Displays information about the IP SLAs responder.
<b>show ip sla standards</b>	Displays information about the IP SLAs standards.
<b>show ip sla statistics</b> [ <i>entry-number</i>   <b>aggregated</b>   <b>details</b> ]	Displays current or aggregated operational status and statistics.

## Configuration Examples for Configuring Cisco IP SLAs Operations

### Configuring an ICMP Echo IP SLAs Operation: Example

This example shows how to configure an ICMP echo IP SLAs operation:

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 60
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
```

```

Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
History Statistics:
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:

```

## Sample Output for Show IP SLA Command: Example

This is an example of the output from the command:

```

Switch# show ip sla application

IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured      : 0
Number of active Entries          : 0
Number of pending Entries         : 0
Number of inactive Entries        : 0

Supported Operation Types
Type of Operation to Perform: 802.lagEcho
Type of Operation to Perform: 802.lagJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224

```

## Configuring a Responder UDP Jitter IP SLAs Operation: Example

This example shows how to configure the device as a responder for the UDP jitter IP SLAs operation in the next procedure:

```

Switch(config)# ip sla responder udp-echo 172.29.139.134 5000

```

## Configuring a UDP Jitter IP SLAs Operation: Example

This example shows how to configure a UDP jitter IP SLAs operation:

```

Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit

```

```

Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
  Operation frequency (seconds): 30
  Next Scheduled Start Time: Pending trigger
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): 3600
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:

```

## Additional References

The following sections provide references related to switch administration:

### Related Documents

Related Topic	Document Title
Cisco IE 2000 commands	<i>Cisco IE 2000 Switch Command Reference</i> , Release 15.0(2)EC
Cisco IOS basic commands	<i>Cisco IOS Configuration Fundamentals Command Reference</i>
IP SLAs commands and configuration	<i>Cisco IOS IP SLAs Configuration Guide</i> on Cisco.com <i>Cisco IOS IP SLAs Command Reference</i> on Cisco.com

### Standards

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

## MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFCs

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

## Technical Assistance

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