



Configuring IP SLAs ICMP Echo Operations

This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. ICMP Echo is useful for troubleshooting network connectivity issues. This module also demonstrates how the results of the ICMP Echo operation can be displayed and analyzed to determine how the network IP connections are performing.

- [Finding Feature Information, page 1](#)
- [Restrictions for IP SLAs ICMP Echo Operations, page 1](#)
- [Information About IP SLAs ICMP Echo Operations, page 2](#)
- [How to Configure IP SLAs ICMP Echo Operations, page 2](#)
- [Configuration Examples for IP SLAs ICMP Echo Operations, page 11](#)
- [Additional References for IP SLAs ICMP Echo Operations, page 11](#)
- [Feature Information for IP SLAs ICMP Echo Operations, page 12](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Restrictions for IP SLAs ICMP Echo Operations

We recommend using a Cisco networking device as the destination device although any networking device that supports RFC 862, Echo protocol, can be used.

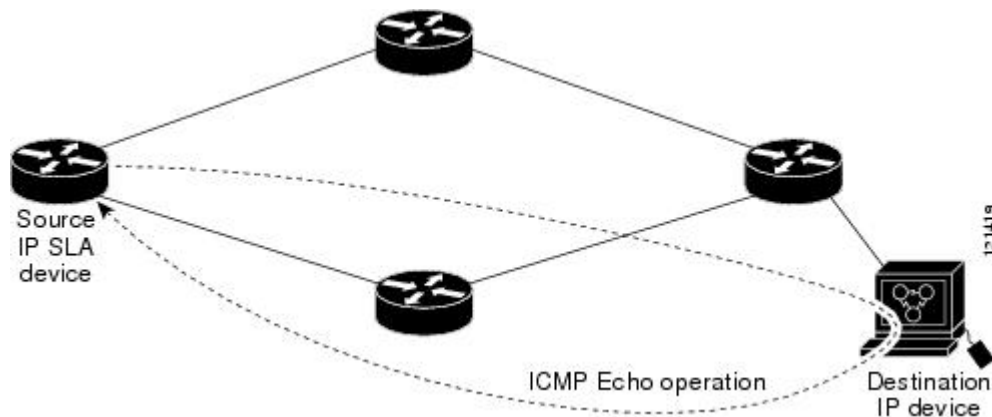
Information About IP SLAs ICMP Echo Operations

ICMP Echo Operation

The ICMP Echo operation measures end-to-end response time between a Cisco router 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.

In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements.

Figure 1: ICMP Echo Operation



The IP SLAs ICMP Echo operation conforms to the same IETF specifications for ICMP ping testing and the two methods result in the same response times.

How to Configure IP SLAs ICMP Echo Operations

Configuring an ICMP Echo Operation



Note

There is no need to configure an IP SLAs responder on the destination device.

Perform one of the following tasks:

Configuring a Basic ICMP Echo Operation on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]
5. **frequency** *seconds*
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip sla <i>operation-number</i> Example: Device(config)# ip sla 6 | Begins configuration for an IP SLAs operation and enters IP SLA configuration mode. |
| Step 4 | icmp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> } source-interface <i>interface-name</i>] Example: Device(config-ip-sla)# icmp-echo 172.29.139.134 | Defines an ICMP Echo operation and enters IP SLA ICMP Echo configuration mode. |
| Step 5 | frequency <i>seconds</i> Example: Device(config-ip-sla-echo)# frequency 300 | (Optional) Sets the rate at which a specified IP SLAs operation repeats. |

| | Command or Action | Purpose |
|---------------|--|--------------------------------|
| Step 6 | end Example: Device(config-ip-sla-echo)# end | Exits to privileged EXEC mode. |

What to Do Next

To add proactive threshold conditions and reactive triggering for generating traps, or for starting another operation, to an IP SLAs operation, see the "Configuring Proactive Threshold Monitoring" section.

Configuring an ICMP Echo Operation with Optional Parameters

Perform this task on the source device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-name*]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** {**none** | **all** | **overThreshold** | **failures**}
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **request-data-size** *bytes*
14. **history statistics-distribution-interval** *milliseconds*
15. **tag** *text*
16. **threshold** *milliseconds*
17. **timeout** *milliseconds*
18. Do one of the following:
 - **tos** *number*
 - **traffic-class** *number*
19. **flow-label** *number*
20. **verify-data**
21. **vrf** *vrf-name*
22. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | <p>ip sla <i>operation-number</i></p> <p>Example:</p> <pre>Device(config)# ip sla 6</pre> | Begins configuration for an IP SLAs operation and enters IP SLA configuration mode. |
| Step 4 | <p>icmp-echo {<i>destination-ip-address</i> <i>destination-hostname</i>} [source-ip {<i>ip-address</i> <i>hostname</i>} source-interface <i>interface-name</i>]</p> <p>Example:</p> <pre>Device(config-ip-sla)# icmp-echo 172.29.139.134 source-ip 172.29.139.132</pre> | Defines an Echo operation and enters IP SLA Echo configuration mode. |
| Step 5 | <p>history buckets-kept <i>size</i></p> <p>Example:</p> <pre>Device(config-ip-sla-echo)# history buckets-kept 25</pre> | (Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation. |
| Step 6 | <p>history distributions-of-statistics-kept <i>size</i></p> <p>Example:</p> <pre>Device(config-ip-sla-echo)# history distributions-of-statistics-kept 5</pre> | (Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation. |
| Step 7 | <p>history enhanced [interval <i>seconds</i>] [buckets <i>number-of-buckets</i>]</p> <p>Example:</p> <pre>Device(config-ip-sla-echo)# history enhanced interval 900 buckets 100</pre> | (Optional) Enables enhanced history gathering for an IP SLAs operation. |
| Step 8 | <p>history filter {none all overThreshold failures}</p> <p>Example:</p> <pre>Device(config-ip-sla-echo)# history filter failures</pre> | (Optional) Defines the type of information kept in the history table for an IP SLAs operation. |
| Step 9 | <p>frequency <i>seconds</i></p> <p>Example:</p> <pre>Device(config-ip-sla-echo)# frequency 30</pre> | (Optional) Sets the rate at which a specified IP SLAs operation repeats. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 10 | history hours-of-statistics-kept <i>hours</i> Example: <pre>Device(config-ip-sla-echo)# history hours-of-statistics-kept 4</pre> | (Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation. |
| Step 11 | history lives-kept <i>lives</i> Example: <pre>Device(config-ip-sla-echo)# history lives-kept 5</pre> | (Optional) Sets the number of lives maintained in the history table for an IP SLAs operation. |
| Step 12 | owner <i>owner-id</i> Example: <pre>Device(config-ip-sla-echo)# owner admin</pre> | (Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation. |
| Step 13 | request-data-size <i>bytes</i> Example: <pre>Device(config-ip-sla-echo)# request-data-size 64</pre> | (Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet. |
| Step 14 | history statistics-distribution-interval <i>milliseconds</i> Example: <pre>Device(config-ip-sla-echo)# history statistics-distribution-interval 10</pre> | (Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation. |
| Step 15 | tag <i>text</i> Example: <pre>Device(config-ip-sla-echo)# tag TelnetPollServer1</pre> | (Optional) Creates a user-specified identifier for an IP SLAs operation. |
| Step 16 | threshold <i>milliseconds</i> Example: <pre>Device(config-ip-sla-echo)# threshold 10000</pre> | (Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation. |
| Step 17 | timeout <i>milliseconds</i> Example: <pre>Device(config-ip-sla-echo)# timeout 10000</pre> | (Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 18 | Do one of the following: <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> Example: <pre>Device(config-ip-sla-jitter)# tos 160</pre> Example: <pre>Device(config-ip-sla-jitter)# traffic-class 160</pre> | (Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation. |
| Step 19 | flow-label <i>number</i> Example: <pre>Device(config-ip-sla-echo)# flow-label 112233</pre> | (Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation. |
| Step 20 | verify-data Example: <pre>Device(config-ip-sla-echo)# verify-data</pre> | (Optional) Causes an IP SLAs operation to check each reply packet for data corruption. |
| Step 21 | vrf <i>vrf-name</i> Example: <pre>Device(config-ip-sla-echo)# vrf vpn-A</pre> | (Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations. |
| Step 22 | end Example: <pre>Device(config-ip-sla-echo)# end</pre> | Exits to privileged EXEC mode. |

What to Do Next

To add proactive threshold conditions and reactive triggering for generating traps, or for starting another operation, to an IP SLAs operation, see the "Configuring Proactive Threshold Monitoring" section.

Scheduling IP SLAs Operations

Before You Begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.
- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh:mm:ss*] [*month day* | *day month*]} | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]
 - **ip sla group schedule** *group-operation-number* *operation-id-numbers* {**schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] [**frequency** *group-operation-frequency*] [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*]} | **pending** | **now** | **after** *hh:mm* [*:ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | Enter one of the following commands: <ul style="list-style-type: none"> • ip sla schedule <i>operation-number</i> [life {forever <i>seconds</i>}] [start-time {[<i>hh:mm:ss</i>] [<i>month day</i> <i>day month</i>]} pending now after <i>hh:mm:ss</i>] [ageout <i>seconds</i>] [recurring] | <ul style="list-style-type: none"> • Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler. |

| | Command or Action | Purpose |
|---------------|--|--|
| | <ul style="list-style-type: none"> • ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> {schedule-period <i>schedule-period-range</i> schedule-together} [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</i>] [life {forever <i>seconds</i>}] [start-time {<i>hh:mm</i> [:<i>ss</i>] [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm</i> [:<i>ss</i>]}] <p>Example:</p> <pre>Device(config)# ip sla schedule 10 life forever start-time now</pre> <pre>Device(config)# ip sla group schedule 10 schedule-period frequency</pre> <pre>Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now</pre> <pre>Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100</pre> | |
| Step 4 | <p>end</p> <p>Example:</p> <pre>Device(config)# end</pre> | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 5 | <p>show ip sla group schedule</p> <p>Example:</p> <pre>Device# show ip sla group schedule</pre> | (Optional) Displays IP SLAs group schedule details. |
| Step 6 | <p>show ip sla configuration</p> <p>Example:</p> <pre>Device# show ip sla configuration</pre> | (Optional) Displays IP SLAs configuration details. |

Troubleshooting Tips

- If the IP Service Level Agreements (SLAs) operation is not running and not generating statistics, add the **verify-data** command to the configuration (while configuring in IP SLA configuration mode) to enable data verification. When data verification is enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.

- Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

To add proactive threshold conditions and reactive triggering for generating traps (or for starting another operation) to an IP Service Level Agreements (SLAs) operation, see the “Configuring Proactive Threshold Monitoring” section.

Configuration Examples for IP SLAs ICMP Echo Operations

Example Configuring an ICMP Echo Operation

The following example shows how to configure an IP SLAs operation type of ICMP Echo that will start immediately and run indefinitely.

```
ip sla 6
 icmp-echo 172.29.139.134 source-ip 172.29.139.132
 frequency 300
 request-data-size 28
 tos 160
 timeout 2000
 tag SFO-RO
 ip sla schedule 6 life forever start-time now
```

Additional References for IP SLAs ICMP Echo Operations

Related Documents

| Related Topic | Document Title |
|---------------------------------|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IP SLAs commands | Cisco IOS IP SLAs Command Reference |
| Information about Cisco IP SLAs | “Cisco IOS IP SLAs Overview” module of the <i>IP SLAs Configuration Guide</i> |

Standards and RFCs

| Standard/RFC | Title |
|--------------|---------------|
| RFC 862 | Echo Protocol |

MIBs

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

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for IP SLAs ICMP Echo Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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/featurenavigator](#). An account on Cisco.com is not required.

Table 1: Feature Information for IP SLAs ICMP Echo Operations

| Feature Name | Releases | Feature Information |
|---|----------------------------|--|
| IP SLAs ICMP Echo Operation | Cisco IOS XE Release 3.2SE | <p>The Cisco IOS IP SLAs Internet Control Message Protocol (ICMP) echo operation allows you to measure end-to-end network response time between a Cisco device and other devices using IP.</p> <p>In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms:</p> <ul style="list-style-type: none"> • Catalyst 3650 Series Switches • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller |
| IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect) | Cisco IOS XE Release 3.2SE | <p>Support was added for operability in IPv6 networks.</p> <p>In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms:</p> <ul style="list-style-type: none"> • Catalyst 3650 Series Switches • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller |

