



EFT REVIEW DRAFT – CISCO CONFIDENTIAL

# Configuring Cisco IOS IP SLAs ICMP Echo Operations

---

**First Published: August 14, 2006**

**Last Updated: February 14, 2011**

This module describes how to configure a Cisco IOS 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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for IP SLAs ICMP Echo Operations”](#) section on page 12.

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.

## Contents

- [Restrictions for IP SLAs ICMP Echo Operations, page 2](#)
- [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](#)
- [Additional References, page 10](#)
- [Feature Information for IP SLAs ICMP Echo Operations, page 12](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2006-2010 Cisco Systems, Inc. All rights reserved.

*EFT REVIEW DRAFT – CISCO CONFIDENTIAL*

# 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

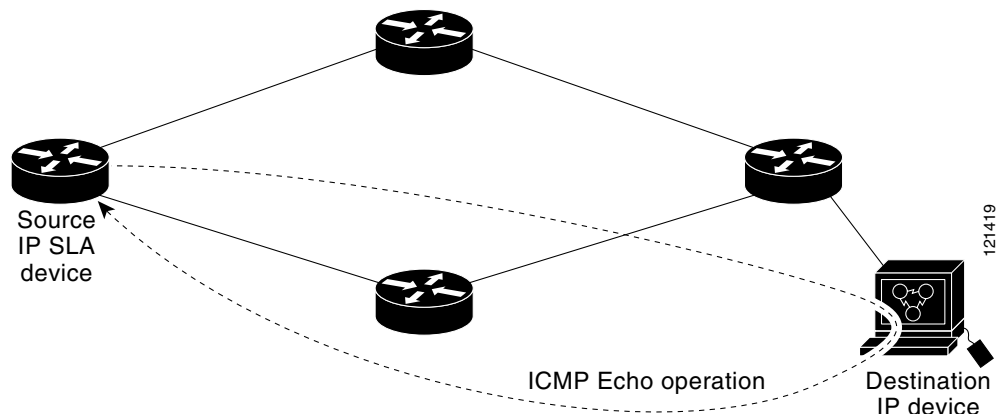
- [ICMP Echo Operation, page 2](#)

## 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 [Figure 1](#) 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, page 3](#) (required)
- [Scheduling IP SLAs Operations, page 7](#)

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

## 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, page 3](#)
- [Configuring an ICMP Echo Operation with Optional Parameters on the Source Device, page 4](#)

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip sla operation-number</b>  <b>Example:</b> Router(config)# ip sla 6	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	<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-name</i> ]  <b>Example:</b> Router(config-ip-sla)# icmp-echo 172.29.139.134	Defines an ICMP Echo operation and enters IP SLA ICMP Echo configuration mode.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 5</b>	<b>frequency</b> <i>seconds</i>  <b>Example:</b> Router(config-ip-sla-echo)# frequency 300	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> Router(config-ip-sla-echo)# end	Exits to privileged EXEC mode.

**Configuring an ICMP Echo Operation with Optional Parameters 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. **tos** *number*  
or  
**traffic-class** *number*
19. **flow-label** *number*
20. **verify-data**
21. **vrf** *vrf-name*
22. **end**

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
<b>Step 3</b>	<p><b>ip sla operation-number</b></p> <p><b>Example:</b> Router(config)# ip sla 6</p>	<p>Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.</p>
<b>Step 4</b>	<p><b>icmp-echo</b> {destination-ip-address   destination-hostname} [<b>source-ip</b> {ip-address   hostname}]   <b>source-interface</b> interface-name]</p> <p><b>Example:</b> Router(config-ip-sla)# icmp-echo 172.29.139.134 source-ip 172.29.139.132</p>	<p>Defines an Echo operation and enters IP SLA Echo configuration mode.</p>
<b>Step 5</b>	<p><b>history buckets-kept size</b></p> <p><b>Example:</b> Router(config-ip-sla-echo)# history buckets-kept 25</p>	<p>(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.</p>
<b>Step 6</b>	<p><b>history distributions-of-statistics-kept size</b></p> <p><b>Example:</b> Router(config-ip-sla-echo)# history distributions-of-statistics-kept 5</p>	<p>(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.</p>
<b>Step 7</b>	<p><b>history enhanced</b> [<b>interval seconds</b>] [<b>buckets number-of-buckets</b>]</p> <p><b>Example:</b> Router(config-ip-sla-echo)# history enhanced interval 900 buckets 100</p>	<p>(Optional) Enables enhanced history gathering for an IP SLAs operation.</p>
<b>Step 8</b>	<p><b>history filter</b> {none   all   overThreshold   failures}</p> <p><b>Example:</b> Router(config-ip-sla-echo)# history filter failures</p>	<p>(Optional) Defines the type of information kept in the history table for an IP SLAs operation.</p>
<b>Step 9</b>	<p><b>frequency seconds</b></p> <p><b>Example:</b> Router(config-ip-sla-echo)# frequency 30</p>	<p>(Optional) Sets the rate at which a specified IP SLAs operation repeats.</p>

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

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

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 18</b>	<pre>tos number</pre> <p>or</p> <pre>traffic-class number</pre> <p><b>Example:</b> Router(config-ip-sla-jitter)# tos 160 or</p> <p><b>Example:</b> Router(config-ip-sla-jitter)# traffic-class 160</p>	<p>(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.</p> <p>or</p> <p>(Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.</p>
<b>Step 19</b>	<pre>flow-label number</pre> <p><b>Example:</b> Router(config-ip-sla-echo)# flow-label 112233</p>	<p>(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.</p>
<b>Step 20</b>	<pre>verify-data</pre> <p><b>Example:</b> Router(config-ip-sla-echo)# verify-data</p>	<p>(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.</p>
<b>Step 21</b>	<pre>vrf vrf-name</pre> <p><b>Example:</b> Router(config-ip-sla-echo)# vrf vpn-A</p>	<p>(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.</p>
<b>Step 22</b>	<pre>end</pre> <p><b>Example:</b> Router(config-ip-sla-echo)# end</p>	<p>Exits to privileged EXEC mode.</p>

## Scheduling IP SLAs Operations

### Restrictions

- The frequency of all operations scheduled in a multioperation group must be the same.
- Operation ID numbers are limited to a maximum of 125 characters. Do not give large integer values as operation ID numbers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

For individual IP SLAs operations only:

3. **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**]

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

For multioperation scheduler only:

4. **ip sla group schedule** *group-operation-number operation-id-numbers*  
**schedule-period** *schedule-period-range* [**ageout** *seconds*] [**frequency** *group-operation-frequency*]  
[**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*month day* | *day month*] | **pending** | **now** |  
**after** *hh:mm:ss*}]
5. **exit**
6. **show ip sla group schedule**
7. **show ip sla configuration**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<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 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> ]  <b>Example:</b> Router(config)# ip sla schedule 6 start-time now life forever	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation.
<b>Step 4</b>	<b>ip sla group schedule</b> <i>group-operation-number operation-id-numbers</i> <b>schedule-period</b> <i>schedule-period-range</i> [ <b>ageout</b> <i>seconds</i> ] [ <b>frequency</b> <i>group-operation-frequency</i> ] [ <b>life</b> { <b>forever</b>   <i>seconds</i> }] [ <b>start-time</b> { <i>hh:mm[:ss]</i> [ <i>month day</i>   <i>day month</i> ]   <b>pending</b>   <b>now</b>   <b>after</b> <i>hh:mm:ss</i> }]	For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode. <ul style="list-style-type: none"> <li>• The frequency of all operations scheduled in the operation group should be the same.</li> <li>• The operation ID numbers are limited to a maximum of 125 characters. Do not use large integer values as operation ID numbers.</li> </ul>
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits to privileged EXEC mode.



**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 6</b>	<b>show ip sla group schedule</b>  <b>Example:</b> Router# show ip sla group schedule	(Optional) Displays the IP SLAs group schedule details.
<b>Step 7</b>	<b>show ip sla configuration</b>  <b>Example:</b> Router# show ip sla configuration	(Optional) Displays the IP SLAs configuration details.

## Examples

The following sample output shows the configuration of all the IP SLAs parameters (including defaults) for the ICMP Echo operation number 6.

```
Router# show ip sla configuration 6

Entry number: 6
Owner: jdoe
Tag: SFO-RO
Type of operation to perform: echo
Target address: 172.29.139.134
Source address: 172.29.139.132
Request size (ARR data portion): 28
Operation timeout (milliseconds): 2000
Type Of Service parameters: 160
Verify data: No
Vrf Name:
Operation frequency (seconds): 300
Next Scheduled Start Time: Start Time already passed
Group Scheduled: FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None
Enhanced History:
```

## Troubleshooting Tips

- If the IP SLAs operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When 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.

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****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 [Configuring Proactive Threshold Monitoring](#).

To view and interpret the results of an IP SLAs operation use the **show ip sla statistics** command. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

**Configuration Examples for IP SLAs ICMP Echo Operations**

- [Example: Configuring an ICMP Echo Operation, page 10](#)

**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****Related Documents**

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Cisco IOS IP SLAs commands	<a href="#">Cisco IOS IP SLAs Command Reference</a>
Cisco IOS IP SLAs: general information	“Cisco IOS IP SLAs Overview” chapter of the <a href="#">Cisco IP SLAs Configuration Guide</a> .

**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.	—

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL****MIBs**

MIBs	MIBs Link
<ul style="list-style-type: none"><li>CISCO-RTTMON-MIB</li><li>IPV6-FLOW-LABEL-MIB</li></ul>	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

RFCs	Title
RFC 862	Echo Protocol

**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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

**EFT REVIEW DRAFT – CISCO CONFIDENTIAL**

# Feature Information for IP SLAs ICMP Echo Operations

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 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.

**Table 1** Feature Information for IP SLAs ICMP Echo Operations

Feature Name	Releases	Feature Information
IP SLAs ICMP Echo Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.0(32)SY 12.3(14)T 15.0(1)S Cisco IOS XE 3.1.0SG	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.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SB 12.2(33)SRC 12.4(20)T Cisco IOS XE 3.1.0SG 12.2(50)SY	Support was added for operability in IPv6 networks.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006-2011 Cisco Systems, Inc. All rights reserved.