



Configuring IP SLAs ICMP Path Echo Operations

Last Updated: March 22, 2011

This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Path Echo operation to monitor end-to-end and hop-by-hop response time between a Cisco router and devices using IP. ICMP Path Echo is useful for determining network availability and for troubleshooting network connectivity issues. The results of the ICMP Path Echo operation can be displayed and analyzed to determine how ICMP is performing.

- [Finding Feature Information, page 1](#)
- [Restrictions for IP SLAs ICMP Path Echo Operations, page 2](#)
- [Information About IP SLAs ICMP Path Echo Operations, page 2](#)
- [How to Configure IP SLAs ICMP Path Echo Operations, page 3](#)
- [Configuration Examples for IP SLAs ICMP Path Echo Operations, page 10](#)
- [Additional References, page 11](#)
- [Feature Information for IP SLAs ICMP Path Echo Operations, page 12](#)
- [, page 12](#)

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 Table at the end of this document.

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.

Restrictions for IP SLAs ICMP Path 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 Path Echo Operations

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

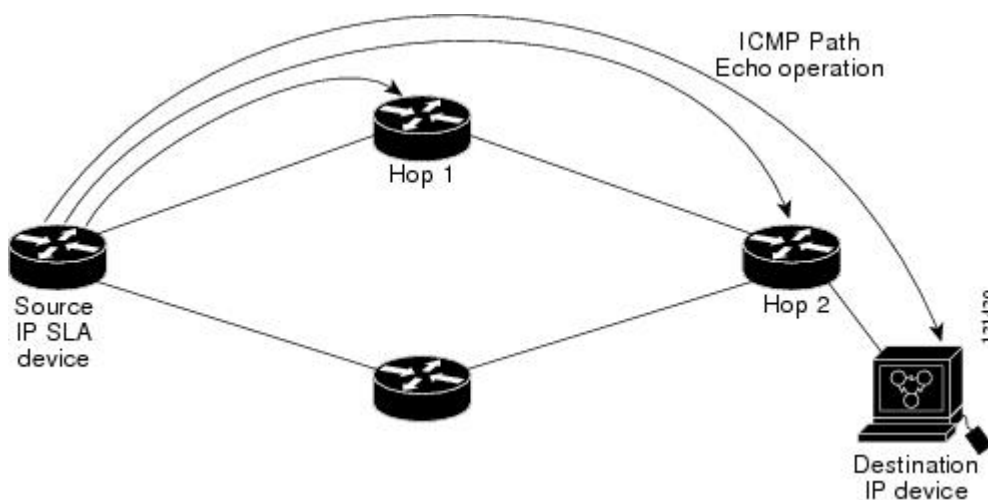
ICMP Path Echo Operation

To monitor ICMP Path Echo performance on a device, use the IP SLAs ICMP Path Echo operation. An ICMP Path Echo operation measures end-to-end and hop-by-hop response time between a Cisco router and devices using IP. ICMP Path Echo is useful for determining network availability and for troubleshooting network connectivity issues.

The IP SLAs ICMP Path Echo operation records statistics for each hop along the path that the IP SLAs operation takes to reach its destination. The ICMP Path Echo operation determines this hop-by-hop response time between a Cisco router and any IP device on the network by discovering the path using the traceroute facility.

In the figure below the source IP SLAs device uses traceroute to discover the path to the destination IP device. A ping is then used to measure the response time between the source IP SLAs device and each subsequent hop in the path to the destination IP device.

Figure 1: ICMP Path Echo Operation



Using the statistics recorded for the response times and availability, the ICMP Path Echo operation can identify a hop in the path that is causing a bottleneck.

How to Configure IP SLAs ICMP Path Echo Operations

- [Configuring an ICMP Path Echo Operation on the Source Device, page 3](#)
- [Scheduling IP SLAs Operations, page 8](#)

Configuring an ICMP Path Echo Operation on the Source Device



Note

This operation does not require an IP SLAs Responder on the destination device.

Perform only one of the following tasks:

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

Configuring a Basic ICMP Path Echo Operation on the Source Device

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-id Example: Router(config)# ip sla 7	Specifies an ID number for the operation being configured, and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	<p>path-echo {<i>destination-ip-address</i> <i>destination-hostname</i>} [source-ip {<i>ip-address</i> <i>hostname</i>}]</p> <p>Example:</p> <pre>Router(config-ip-sla)# path-echo protocol 172.29.139.134</pre>	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.
Step 5	<p>frequency <i>seconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	<p>end</p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# end</pre>	Exits to privileged EXEC mode.

Example

The following example shows the configuration of the IP SLAs ICMP Path Echo operation number 7 that will start in 30 seconds and run for 5 minutes.

```
ip sla 7
 path-echo 172.29.139.134
 frequency 30
!
ip sla schedule 7 start-time after 00:00:30 life 300
```

Configuring an ICMP Path Echo Operation with Optional Parameters on the Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **path-echo** { *destination-ip-address* | *destination-hostname* } [**source-ip** { *ip-address* | *hostname* }]
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. **paths-of-statistics-kept** *size*
14. **request-data-size** *bytes*
15. **samples-of-history-kept** *samples*
16. **history statistics-distribution-interval** *milliseconds*
17. **tag** *text*
18. **threshold** *milliseconds*
19. **timeout** *milliseconds*
20. **tos** *number*
21. **verify-data**
22. **vrf** *vrf-name*
23. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Router(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

	Command or Action	Purpose
Step 4	<p>path-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> }]</p> <p>Example:</p> <pre>Router(config-ip-sla)# path-echo 172.29.139.134</pre>	Defines a Path Echo operation and enters IP SLA Path Echo configuration mode.
Step 5	<p>history buckets-kept <i>size</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# 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>Router(config-ip-sla-pathEcho)# 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 [<i>interval seconds</i>] [buckets <i>number-of-buckets</i>]</p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# 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>Router(config-ip-sla-pathEcho)# 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>Router(config-ip-sla-pathEcho)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	<p>history hours-of-statistics-kept <i>hours</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# 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	<p>history lives-kept <i>lives</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# history lives-kept 5</pre>	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.

	Command or Action	Purpose
Step 12	<p>owner <i>owner-id</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	<p>paths-of-statistics-kept <i>size</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# paths-of-statistics-kept 3</pre>	(Optional) Sets the number of paths for which statistics are maintained per hour for an IP SLAs operation.
Step 14	<p>request-data-size <i>bytes</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# request-data-size 64</pre>	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	<p>samples-of-history-kept <i>samples</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# samples-of-history-kept 10</pre>	(Optional) Sets the number of entries kept in the history table per bucket for an IP SLAs operation.
Step 16	<p>history statistics-distribution-interval <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# history statistics-distribution-interval 10</pre>	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 17	<p>tag <i>text</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# tag TelnetPollServer1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 18	<p>threshold <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 19	<p>timeout <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-pathEcho)# timeout 10000</pre>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 20	<p>tos <i>number</i></p>	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.

	Command or Action	Purpose
	Example: Router(config-ip-sla-pathEcho)# tos 160	
Step 21	verify-data Example: Router(config-ip-sla-pathEcho)# verify-data	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	vrf vrf-name Example: Router(config-ip-sla-pathEcho)# vrf vpn-A	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 23	end Example: Router(config-ip-sla-pathEcho)# end	Exits to privileged EXEC mode.

Scheduling IP SLAs Operations



Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
 - **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* [**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. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>Do one of the following:</p> <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] ip sla group schedule <i>group-operation-number</i> <i>operation-id-numbers</i> schedule-period <i>schedule-period-range</i> [ageout <i>seconds</i>] [frequency <i>group-operation-frequency</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>}] <p>Example:</p> <pre>Router(config)# ip sla schedule 10 start-time now life forever</pre> <p>Example:</p> <pre>Router(config)# ip sla group schedule 1 3,4,6-9</pre>	<p>For individual IP SLAs operations only:</p> <p>Configures the scheduling parameters for an individual IP SLAs operation.</p> <p>or</p> <p>For multioperation scheduler only:</p> <p>Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.</p>
Step 4	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits to privileged EXEC mode.</p>
Step 5	<p>show ip sla group schedule</p> <p>Example:</p> <pre>Router# show ip sla group schedule</pre>	<p>(Optional) Displays the IP SLAs group schedule details.</p>
Step 6	<p>show ip sla configuration</p> <p>Example:</p> <pre>Router# show ip sla configuration</pre>	<p>(Optional) Displays the IP SLAs configuration details.</p>

- [Troubleshooting Tips](#), page 10
- [What to Do Next](#), page 10

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 **debugipsla 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 SLAs operation, see the "Configuring Proactive Threshold Monitoring" section.

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.

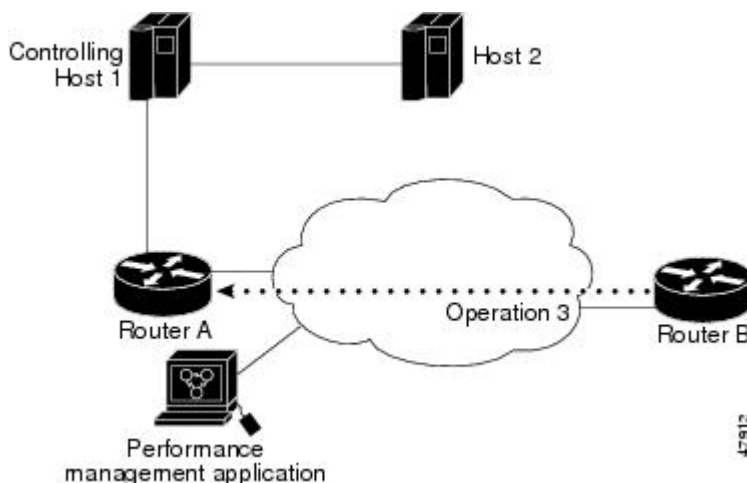
Configuration Examples for IP SLAs ICMP Path Echo Operations

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

Example Configuring an ICMP Path Echo Operation

The following example shows how to configure an IP SLAs operation type of ICMP Path Echo that will start after 30 seconds and run for 5 minutes. The figure below depicts the ICMP Path Echo operation.

Figure 2: ICMP Path Echo Operation



This example sets a Path Echo operation (ip sla 3) from Router B to Router A using IP/ICMP. The operation attempts to execute three times in 25 seconds (first attempt at 0 seconds).

Router B Configuration

```
ip sla 3
  path-echo 172.29.139.134
  frequency 10
  tag SGN-RO
  timeout 1000
ip sla schedule 3 life 25
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	<i>Cisco IOS IP SLAs Command Reference</i>

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
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

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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP SLAs ICMP Path 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/cfn>. An account on Cisco.com is not required.

Table 1: Feature Information for the IP SLAs ICMP Path Echo Operation

Feature Name	Releases	Feature Information
IP SLAs ICMP Path Echo Operation	Cisco IOS XE Release 2.1	The IP SLAs Internet Control Message Protocol (ICMP) path echo operation allows you to measure end-to-end and hop-by-hop network response time between a Cisco device and other devices using IP.

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. 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 and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.