



Configuring IP SLAs UDP Echo Operations

Last Updated: March 31, 2011

This module describes how to configure an IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. UDP echo accuracy is enhanced by using the IP SLAs Responder at the destination Cisco router. This module also demonstrates how the results of the UDP echo operation can be displayed and analyzed to determine how a UDP application is performing.

- [Finding Feature Information, page 1](#)
- [Restrictions for IP SLAs UDP Echo Operations, page 1](#)
- [Information About IP SLAs UDP Echo Operations, page 2](#)
- [How to Configure IP SLAs UDP Echo Operations, page 2](#)
- [Configuration Examples for IP SLAs UDP Echo Operations, page 11](#)
- [Additional References, page 11](#)
- [Feature Information for the IP SLAs UDP Echo Operation, 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IP SLAs UDP 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 UDP Echo Operations

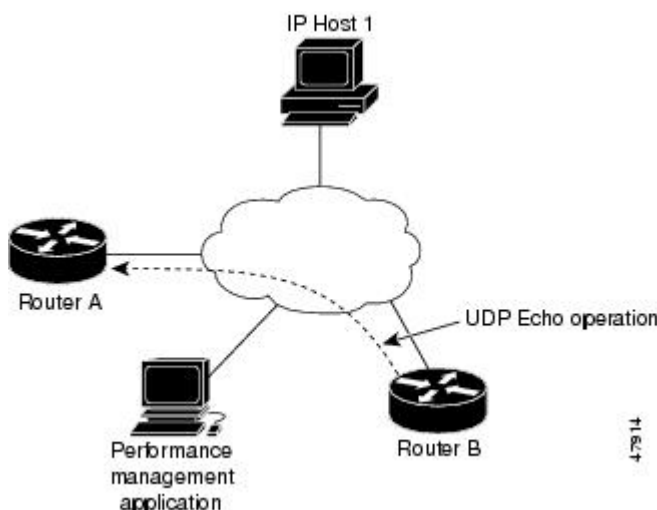
- [UDP Echo Operation, page 2](#)

UDP Echo Operation

The UDP echo operation measures end-to-end response time between a Cisco router and devices using IP. UDP is a transport layer (Layer 4) Internet protocol that is used for many IP services. UDP echo is used to measure response times and test end-to-end connectivity.

In the figure below Router A has been configured as an IP SLAs Responder and Router B is configured as the source IP SLAs device.

Figure 1: UDP Echo Operation



Response time (round-trip time) is computed by measuring the time taken between sending a UDP echo request message from Router B to the destination router--Router A--and receiving a UDP echo reply from Router A. UDP echo accuracy is enhanced by using the IP SLAs Responder at Router A, the destination Cisco router. If the destination router is a Cisco router, then IP SLAs sends a UDP datagram to any port number that you specified. Using the IP SLAs Responder is optional for a UDP echo operation when using Cisco devices. The IP SLAs Responder cannot be configured on non-Cisco devices.

The results of a UDP echo operation can be useful in troubleshooting issues with business-critical applications by determining the round-trip delay times and testing connectivity to both Cisco and non-Cisco devices.

How to Configure IP SLAs UDP Echo Operations

- [Configuring the IP SLAs Responder on the Destination Device, page 3](#)

- [Configuring a UDP Echo Operation on the Source Device, page 4](#)
- [Scheduling IP SLAs Operations, page 8](#)

Configuring the IP SLAs Responder on the Destination Device

If you are using the IP SLAs Responder, ensure that the networking device to be used as the responder is a Cisco device and that you have connectivity to that device through the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress *ip-address* port *port***
4. **exit**

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	Do one of the following: <ul style="list-style-type: none"> • ip sla responder • ip sla responder udp-echo ipaddress <i>ip-address</i> port <i>port</i> Example: Router(config)# ip sla responder Example: Router(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000	(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source. or (Optional) Required only if protocol control is disabled on source. Permanently enables IP SLAs Responder functionality on specified IP address and port. <ul style="list-style-type: none"> • Control is enabled by default.
Step 4	exit Example: Router(config)# exit	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring a UDP Echo Operation on the Source Device

Perform only one of the following tasks:

- [Configuring a Basic UDP Echo Operation on the Source Device, page 4](#)
- [Configuring a UDP Echo Operation with Optional Parameters on the Source Device, page 5](#)

Configuring a Basic UDP Echo Operation on the Source Device

If you are using the IP SLAs Responder, ensure that you have completed the "Configuring the IP SLAs Responder on the Destination Device" section before you start this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
5. **frequency** *seconds*
6. **exit**

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-number Example: Router(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	udp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> } <i>destination-port</i> [source-ip { <i>ip-address</i> <i>hostname</i> } source-port <i>port-number</i>] [control { enable disable }] Example: Router(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. <ul style="list-style-type: none"> • Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.

	Command or Action	Purpose
Step 5	frequency <i>seconds</i> Example: Router(config-ip-sla-udp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	exit Example: Router(config-ip-sla-udp)# exit	Exits IP SLA UDP configuration mode and returns to global configuration mode.

Configuring a UDP Echo Operation with Optional Parameters on the Source Device

If you are using the IP SLAs Responder, ensure that you have completed the "Configuring the IP SLAs Responder on the Destination Device" section before you start this task.

SUMMARY STEPS

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

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>ip sla <i>operation-number</i></p> <p>Example:</p> <pre>Router(config)# ip sla 10</pre>	<p>Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.</p>
Step 4	<p>udp-echo {<i>destination-ip-address</i> <i>destination-hostname</i>} <i>destination-port</i> [source-ip {<i>ip-address</i> <i>hostname</i>} source-port <i>port-number</i>] [control {enable disable}]</p> <p>Example:</p> <pre>Router(config-ip-sla)# udp-echo 172.29.139.134 5000</pre>	<p>Defines a UDP echo operation and enters IP SLA UDP configuration mode.</p> <ul style="list-style-type: none"> Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	<p>history buckets-kept <i>size</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# history buckets-kept 25</pre>	<p>(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.</p>
Step 6	<p>data-pattern <i>hex-pattern</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# data-pattern</pre>	<p>(Optional) Specifies the data pattern in an IP SLAs operation to test for data corruption.</p>
Step 7	<p>history distributions-of-statistics-kept <i>size</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# history distributions- of-statistics-kept 5</pre>	<p>(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.</p>
Step 8	<p>history enhanced [<i>interval seconds</i>] [buckets <i>number-of-buckets</i>]</p>	<p>(Optional) Enables enhanced history gathering for an IP SLAs operation.</p>

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-ip-sla-udp)# history enhanced interval 900 buckets 100</pre>	
Step 9	<p>history filter { none all overThreshold failures }</p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# history filter failures</pre>	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	<p>frequency <i>seconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	<p>history hours-of-statistics-kept <i>hours</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# history hours-of- statistics-kept 4</pre>	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 12	<p>history lives-kept <i>lives</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# history lives-kept 5</pre>	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	<p>owner <i>owner-id</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	<p>request-data-size <i>bytes</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# 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>history statistics-distribution-interval <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# history statistics- distribution-interval 10</pre>	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	<p>tag <i>text</i></p>	(Optional) Creates a user-specified identifier for an IP SLAs operation.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-ip-sla-udp)# tag TelnetPollServer1</pre>	
Step 17	<p>threshold <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	<p>timeout <i>milliseconds</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# timeout 10000</pre>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	<p>Do one of the following:</p> <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# tos 160</pre> <p>Example:</p> <pre>Router(config-ip-sla-jitter)# traffic-class 160</pre>	<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>
Step 20	<p>flow-label <i>number</i></p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# 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 21	<p>verify-data</p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# verify-data</pre>	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	<p>exit</p> <p>Example:</p> <pre>Router(config-ip-sla-udp)# exit</pre>	Exits UDP configuration submenu and returns to global configuration 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	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	Do one of the following: <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>}] 	For individual IP SLAs operations only: Configures the scheduling parameters for an individual IP SLAs operation. or For multioperation scheduler only: Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.

	Command or Action	Purpose
	<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>	
Step 4	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.
Step 5	<p>show ip sla group schedule</p> <p>Example:</p> <pre>Router# show ip sla group schedule</pre>	(Optional) Displays the IP SLAs group schedule details.
Step 6	<p>show ip sla configuration</p> <p>Example:</p> <pre>Router# show ip sla configuration</pre>	(Optional) Displays the IP SLAs configuration details.

- [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 UDP Echo Operations

- [Example Configuring a UDP Echo Operation, page 11](#)

Example Configuring a UDP Echo Operation

The following example configures an IP SLAs operation type of UDP echo that will start immediately and run indefinitely.

```
ip sla 5
  udp-echo 172.29.139.134 5000
  frequency 30
  request-data-size 160
  tos 128
  timeout 1000
  tag FLL-RO
ip sla schedule 5 life forever start-time now
```

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 the IP SLAs UDP Echo Operation

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for the IP SLAs UDP Echo Operation

Feature Name	Releases	Feature Information
IP SLAs UDP Jitter Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.3(14)T 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs User Datagram Protocol (UDP) jitter operation allows you to measure round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SRC 12.2(33)SB 12.4(20)T Cisco IOS XE 3.1.0SG	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. 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.