



Configuring IP SLAs UDP Echo Operations

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 device and devices using IPv4 or IPv6. UDP echo accuracy is enhanced by using the Cisco IP SLAs Responder at the destination Cisco device. 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 3](#)
- [Configuration Examples for IP SLAs UDP Echo Operations, page 12](#)
- [Additional References, page 12](#)
- [Feature Information for the IP SLAs UDP Echo Operation, page 13](#)

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 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.

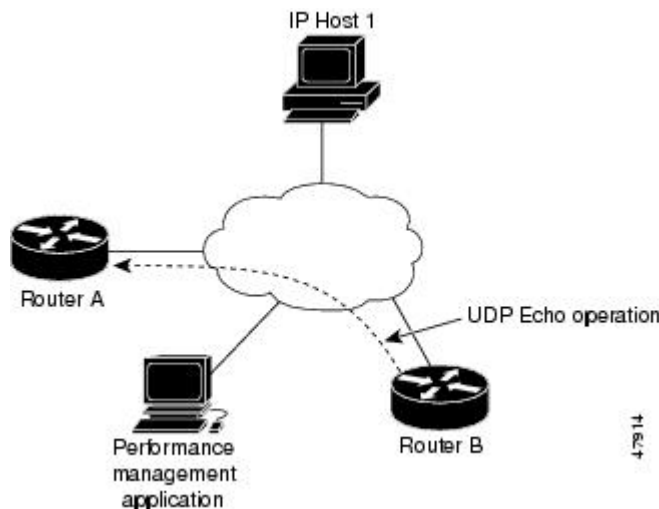
Information About IP SLAs UDP Echo Operations

UDP Echo Operation

The UDP echo operation measures end-to-end response time between a Cisco device 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 Device A has been configured as an IP SLAs Responder and Device 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 Device B to the destination device--Device A--and receiving a UDP echo reply from Device A. UDP echo accuracy is enhanced by using the IP SLAs Responder at Device A, the destination Cisco device. If the destination device is a Cisco device, 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 a Destination Device

**Note**

A responder should not configure a permanent port for a sender. If the responder configures a permanent port for a sender, even if the packets are successfully sent (no timeout or packet-loss issues), the jitter value is zero.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip sla responder**
 - **ip sla responder udp-echo ipaddress *ip-address* port *port* vrf *vrf***
4. **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.
Step 3	Enter one of the following commands: • ip sla responder • ip sla responder udp-echo ipaddress <i>ip-address</i> port <i>port</i> vrf <i>vrf</i>	(Optional) Temporarily enables IP SLAs responder functionality on a Cisco device in response to control messages from the source. (Optional; required only if protocol control is disabled on the source.) Enables IP SLAs responder functionality on the specified IP address, port and VRF.

	Command or Action	Purpose
	Example: <pre>Device(config)# ip sla responder</pre> <pre>Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000 vrf vrf1</pre>	Protocol control is enabled by default.
Step 4	end Example: <pre>Device(config)# end</pre>	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

Before You Begin

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. **data-pattern** *hex value*
6. **frequency** *seconds*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	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 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> [<i>source-ip</i> {<i>ip-address</i> <i>hostname</i>} <i>source-port</i> <i>port-number</i>] [<i>control</i> {<i>enable</i> <i>disable</i>}] Example: Device(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target devices.
Step 5	data-pattern <i>hex value</i> Example: Device(config-ip-sla-udp)# data-pattern FFFFFFFF	(Optional) Sets a hexadecimal value for data pattern. The range is 0 to FFFFFFFF.
Step 6	frequency <i>seconds</i> Example: Device(config-ip-sla-udp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 7	end Example: Device(config-ip-sla-udp)# end	Returns 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 a UDP Echo Operation with Optional Parameters on the Source Device

Before You Begin

If you are using an IP SLAs Responder in this operation, the responder must be configured on the destination device. See the "Configuring the IP SLAs Responder on the Destination Device."

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	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	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 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: Device(config-ip-sla)# udp-echo 172.29.139.134 5000	Defines a UDP echo operation and enters IP SLA UDP configuration mode. Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target devices.
Step 5	history buckets-kept <i>size</i> Example: Device(config-ip-sla-udp)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	data-pattern <i>hex-pattern</i> Example: Device(config-ip-sla-udp)# data-pattern	(Optional) Specifies the data pattern in an IP SLAs operation to test for data corruption.
Step 7	history distributions-of-statistics-kept <i>size</i> Example: Device(config-ip-sla-udp)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.

	Command or Action	Purpose
Step 8	history enhanced [interval <i>seconds</i>] [buckets <i>number-of-buckets</i>] Example: <pre>Device(config-ip-sla-udp)# history enhanced interval 900 buckets 100</pre>	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 9	history filter {none all overThreshold failures} Example: <pre>Device(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	frequency <i>seconds</i> Example: <pre>Device(config-ip-sla-udp)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	history hours-of-statistics-kept <i>hours</i> Example: <pre>Device(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	history lives-kept <i>lives</i> Example: <pre>Device(config-ip-sla-udp)# history lives-kept 2</pre>	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	owner <i>owner-id</i> Example: <pre>Device(config-ip-sla-udp)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	request-data-size <i>bytes</i> Example: <pre>Device(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	history statistics-distribution-interval <i>milliseconds</i> Example: <pre>Device(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.

	Command or Action	Purpose
Step 16	tag <i>text</i> Example: <pre>Device(config-ip-sla-udp)# tag TelnetPollServer1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 17	threshold <i>milliseconds</i> Example: <pre>Device(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	timeout <i>milliseconds</i> Example: <pre>Device(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	Do one of the following: • 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 20	flow-label <i>number</i> Example: <pre>Device(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	verify-data Example: <pre>Device(config-ip-sla-udp)# verify-data</pre>	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 22	exit Example: <pre>Device(config-ip-sla-udp)# exit</pre>	Exits UDP configuration submode and returns to global configuration 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. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: • 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> 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>]}] Example: Device(config)# ip sla schedule 10 life forever start-time now Device(config)# ip sla group schedule 10 schedule-period frequency Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100	• 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.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	show ip sla group schedule Example: Device# show ip sla group schedule	(Optional) Displays IP SLAs group schedule details.
Step 6	show ip sla configuration Example: Device# show ip sla configuration	(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 UDP Echo Operations

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	Cisco IOS IP SLAs Command Reference

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 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 Echo Operation	Cisco IOS 12.2(31)SB2 Cisco IOS 12.2(33)SRB1 Cisco IOS 12.2(33)SXH Cisco IOS 12.3(14)T Cisco IOS XE Release 2.1 Cisco IOS 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)	Cisco IOS 12.2(33)SRC Cisco IOS 12.2(33)SB Cisco IOS 12.4(20)T Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG Cisco IOS 12.2(50)SY	Support was added for operability in IPv6 networks.