Configuring IP SLAs UDP Echo Operations

This chapter 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 switch and devices using IPv4. UDP echo accuracy is enhanced by using the IP SLAs Responder at the destination Cisco switch. 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.

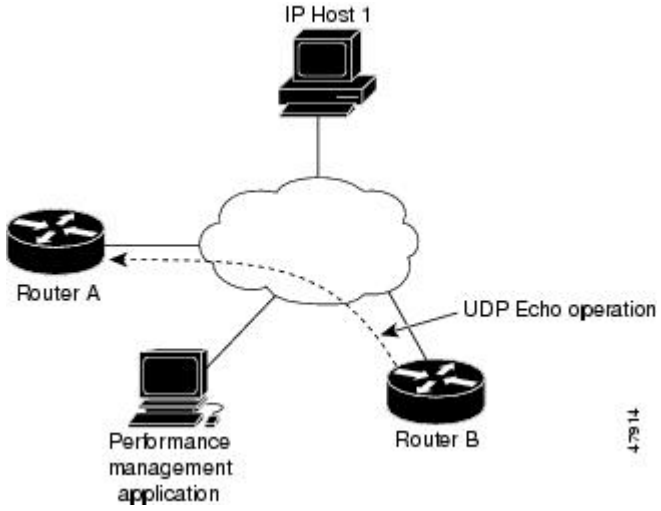
This chapter includes the following sections:

- UDP Echo Operation, on page 1
- Guidelines and Limitations for UDP Echo Operations, on page 2
- Configuring the IP SLAs Responder on the Destination Device, on page 4
- Configuring a Basic UDP Echo Operation on the Source Device, on page 5
- Configuring a UDP Echo Operation with Optional Parameters on the Source Device, on page 6
- Scheduling IP SLAs Operations, on page 10
- Configuration Example for a UDP Echo Operation, on page 12

UDP Echo Operation

The UDP echo operation measures end-to-end response time between a Cisco switch 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 following figure, Switch A is configured as an IP SLAs Responder and Switch B is configured as the source IP SLAs device.



The response time (round-trip time) is computed by measuring the time taken between sending a UDP echo request message from Switch B to the destination switch--Switch A--and receiving a UDP echo reply from Switch A. UDP echo accuracy is enhanced by using the responder at Switch A, the destination Cisco switch. If the destination switch is a Cisco switch, the IP SLAs Responder 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.

Guidelines and Limitations for UDP Echo Operations

- **show** commands with the **internal** keyword are not supported.

Configuring CoPP for IP SLA Packets

When using IP SLA operations on a large scale, a specific CoPP configuration to allow the IP SLA packets to pass through might be needed. Because IP SLA uses user-defined UDP ports, there is no way to allow all IP SLA packets to the control plane. However, you can specify each destination/source port that IP SLA can use.

For more information about the verified scalability of the number of IP SLA probes, see the *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*.

The following CoPP configuration example allows IP SLA packets to pass through. It assumes destination ports and source ports in the range of 6500-7000. In this example, if “insert-before” is not specified, "copp-ipsla" will be added after “class-default.”

Note The following configuration example might vary based on platform/hardware type. Please refer to the Cisco Nexus 9000 Series NX-OS Security Configuration Guide for details about configuring IP ACL and CoPP.

```
ip access-list acl-sla-allow
  10 remark ### ALLOW SLA control packets from 1.1.1.0/24
  20 permit udp 1.1.1.0/24 any eq 1967
  30 remark ### ALLOW SLA data packets from 1.1.1.0/24 using ports 6500-7000
  40 permit udp 1.1.1.0/24 any range 6500 7000

class-map type control-plane match-any copp-ipsla
  match access-group name acl-sla-allow

policy-map type control-plane Custom-copp-policy-strict
    class copp-ipsla insert-before Custom-copp-class-l2-default
    police cir 1500 kbps

control-plane
  service-policy input Custom-copp-policy-strict

switch# show policy-map interface control-plane | be copp-ipsla
    class-map copp-ipsla (match-any)
      match access-group name acl-sla-allow
      set cos 7
      police cir 1500 kbps , bc 32000 bytes
      module 1 :
        transmitted 0 bytes;
        dropped 0 bytes;

    class-map Custom-copp-class-l2-default (match-any)
      match access-group name Custom-copp-acl-mac-undesirable
      set cos 0
      police cir 400 kbps , bc 32000 bytes
      module 1 :
        transmitted 0 bytes;
        dropped 0 bytes;

    class-map class-default (match-any)
      set cos 0
      police cir 400 kbps , bc 32000 bytes
      module 1 :
        transmitted 122 bytes;
        dropped 0 bytes;
```

Matching the Netstack Port Range

IP SLA only accepts ports within the local netstack port range. The source and destination ports used in the probe's configuration must match the supported netstack ports on the SLA sender and the SLA responder.

When performing ISSU from earlier versions to version 9.3(1) and later versions, ensure that the features with user-defined ports, such as SSH port, are within the range mentioned in the following table.

Table 1: Port Range for ISSU

Version	Default port-range
9.3(1)	Kstack local port range (15001 - 58000) Netstack local port range (58001 - 63535) nat port range (63536 - 65535)

Version	Default port-range
9.3(2)	Kstack local port range (15001 - 58000) Netstack local port range (58001 - 63535) nat port range (63536 - 65535)
9.3(3) onwards	Kstack local port range (15001 - 58000) Netstack local port range (58001 - 60535) nat port range (60536 - 65535)

You can use the **show sockets local-port-range** command to view the port range on the sender/responder.

The following is an example of viewing the netstack port range:

```
switch# show sockets local-port-range

Kstack local port range (15001 - 22002)
Netstack local port range (22003 - 65535)
```

Configuring the IP SLAs Responder on the Destination Device

Before you begin

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. **feature sla responder**
4. Do one of the following:
   - **ip sla responder**

     Example:

     ```
     switch(config)# ip sla responder
     ```
   - **ip sla responder udp-echo ipaddress** *ip-address* **port** *port*

     Example:

     ```
     switch(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000
     ```
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode Enter your password if prompted.
Step 2	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 3	**feature sla responder** **Example:** `switch(config)# feature sla responder`	Enables the IP SLAs responder feature.

Step 4	Do one of the following:
	• **ip sla responder**
	Example:
	`switch(config)# ip sla responder`
	• **ip sla responder udp-echo ipaddress** *ip-address* **port** *port*
	Example:
	`switch(config)# ip sla responder udp-echo ipaddress 172.29.139.132 port 5000`
		-
		• Temporarily enables the IP SLAs Responder functionality on a Cisco device in response to control messages from the source.
		• Required only if the protocol control is disabled on the source. This command permanently enables the IP SLAs Responder functionality on a specified IP address and port.
		Control is enabled by default.

Step 5	**exit** **Example:** `switch(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Basic UDP Echo Operation on the Source Device

This section describes how to configure a basic UDP echo operation on the source.

Note 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.

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*} **sourceport** *port-number*] [**control** {**enable** | **disable**}]
5. (Optional) **frequency** *seconds*
6. (Optional) **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `switch(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **sourceport** *port-number*] [**control** {**enable** | **disable**}] **Example:** `switch(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 switches.
Step 5	(Optional) **frequency** *seconds* **Example:** `switch(config-ip-sla-udp)# frequency 30`	Sets the rate at which a specified IP SLAs operation repeats.
Step 6	(Optional) **end** **Example:** `switch(config-ip-sla-udp)# end`	Returns to privileged EXEC mode.

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

This section describes how to configure a UDP echo operation with optional parameters on the source device.

Note 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.

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" section.

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*} **sourceport** *port-number*] [**control** {**enable** | **disable**}]
5. (Optional) **history buckets-kept** *size*
6. (Optional) **data-pattern** *hex-pattern*
7. (Optional) **history distributions-of-statistics-kept** *size*
8. (Optional) **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
9. (Optional) **history filter** {**none** | **all** | **overThreshold** | **failures**}
10. (Optional) **frequency** *seconds*
11. (Optional) **history hours-of-statistics-kept** *hours*
12. (Optional) **history lives-kept** *lives*
13. (Optional) **owner** *owner-id*
14. (Optional) **request-data-size** *bytes*
15. (Optional) **history statistics-distribution-interval** *milliseconds*
16. (Optional) **tag** *text*
17. (Optional) **threshold** *milliseconds*
18. (Optional) **timeout** *milliseconds*
19. (Optional) **tos** *number*
20. (Optional) **verify-data**
21. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip sla** *operation-number* **Example:** `switch(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**udp-echo** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **sourceport** *port-number*] [**control** {**enable** | **disable**}] **Example:** `switch(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 switches.
Step 5	(Optional) **history buckets-kept** *size* **Example:** `switch(config-ip-sla-udp)# history buckets-kept 25`	Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	(Optional) **data-pattern** *hex-pattern* **Example:** `switch(config-ip-sla-udp)# data-pattern`	Specifies the data pattern in an IP SLAs operation to test for data corruption.
Step 7	(Optional) **history distributions-of-statistics-kept** *size* **Example:** `switch(config-ip-sla-udp)# history distributionsof- statistics-kept 5`	Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 8	(Optional) **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `switch(config-ip-sla-udp)# history enhanced interval 900 buckets 100`	Enables enhanced history gathering for an IP SLAs operation.
Step 9	(Optional) **history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `switch(config-ip-sla-udp)# history filter failures`	Defines the type of information kept in the history table for an IP SLAs operation.
Step 10	(Optional) **frequency** *seconds* **Example:** `switch(config-ip-sla-udp)# frequency 30`	Sets the rate at which a specified IP SLAs operation repeats.
Step 11	(Optional) **history hours-of-statistics-kept** *hours* **Example:** `switch(config-ip-sla-udp)# history hours-ofstatistics- kept 4`	Sets the number of hours for which statistics are maintained for an IP SLAs operation.

	Command or Action	Purpose
Step 12	(Optional) **history lives-kept** *lives* **Example:** `switch(config-ip-sla-udp)# history lives-kept 5`	Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 13	(Optional) **owner** *owner-id* **Example:** `switch(config-ip-sla-udp)# owner admin`	Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 14	(Optional) **request-data-size** *bytes* **Example:** `switch(config-ip-sla-udp)# request-data-size 64`	Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 15	(Optional) **history statistics-distribution-interval** *milliseconds* **Example:** `switch(config-ip-sla-udp)# history statistics distribution- interval 10`	Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 16	(Optional) **tag** *text* **Example:** `switch(config-ip-sla-udp)# tag TelnetPollServer1`	Creates a user-specified identifier for an IP SLAs operation.
Step 17	(Optional) **threshold** *milliseconds* **Example:** `switch(config-ip-sla-udp)# threshold 10000`	Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 18	(Optional) **timeout** *milliseconds* **Example:** `switch(config-ip-sla-udp)# timeout 10000`	Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 19	(Optional) **tos** *number* **Example:** `switch(config-ip-sla-jitter)# tos 160`	In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 20	(Optional) **verify-data** **Example:** `switch(config-ip-sla-udp)# verify-data`	Causes an IP SLAs operation to check each reply packet for data corruption.
Step 21	**exit** **Example:** `switch(config-ip-sla-udp)# exit`	Exits UDP configuration submode and returns to global configuration mode.

Scheduling IP SLAs Operations

This section describes how to schedule IP SLAs operations.

Before you begin

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.
- The 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 (,).

Tip

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ip sla schedule** *operation-number* [**life forever** { | *seconds*}] [**starttime** {*hh : mm*[: *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh : mm : ss*}] [**ageout** *seconds*] [**recurring**]

     Example:

     ```
     ip sla schedule operation-number [life {forever | seconds}] [starttime {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*}] [**starttime**{ *hh:mm*[:*ss*] [*month day* | *day month]* | **pending** | **now** | **after** *hh:mm:ss*}]

     Example:

     ```
     switch(config)# ip sla group schedule 1 3,4,6-9
     ```

4. **exit**
5. **show ip sla group schedule**
6. **show ip sla configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.

Step 3	Do one of the following:
	• **ip sla schedule** *operation-number* [**life forever** { | *seconds*}] [**starttime** {*hh : mm*[: *ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh : mm : ss*}] [**ageout** *seconds*] [**recurring**]
	Example:
	`ip sla schedule operation-number [life {forever | seconds}] [starttime {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*}] [**starttime**{ *hh:mm*[:*ss*] [*month day* | *day month]* | **pending** | **now** | **after** *hh:mm:ss*}]
	Example:
	`switch(config)# ip sla group schedule 1 3,4,6-9`
		-
		• For individual IP SLAs operations only:
		Configures the scheduling parameters for an individual IP SLAs operation.
		• For the multioperations scheduler only:
		Specifies an IP SLAs operation group number and the range of operation numbers to be scheduled in global configuration mode.

Step 4	**exit** **Example:** `switch(config)# exit`	Exits to privileged EXEC mode.
Step 5	**show ip sla group schedule** **Example:** `switch# show ip sla group schedule`	(Optional) Displays the IP SLAs group schedule details.
Step 6	**show ip sla configuration** **Example:** `switch# show ip sla configuration`	(Optional) Displays the IP SLAs configuration details.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps or for starting another 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 Example for a UDP Echo Operation

This example shows how to configure an IP SLAs operation type of UDP echo that starts immediately and runs 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
```