Configuring IP SLAs UDP Jitter Operations

This chapter describes how to configure an IP Service Level Agreements (SLAs) UDP jitter operation to analyze round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic in IPv4 networks. This chapter also demonstrates how the data gathered using the UDP jitter operation can be displayed and analyzed using the Cisco software commands.

This chapter includes the following sections:

Information About the IP SLAs UDP Jitter Operation

The IP SLAs UDP jitter operation can diagnose network suitability for real-time traffic applications such as voice over IP (VoIP), video over IP, or real-time conferencing.

Jitter means inter-packet delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (such as queuing, arriving through alternate routes, and so on), the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived greater than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks such as VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal.

However, the IP SLAs UDP jitter operation does more than just monitor jitter. As the UDP jitter operation includes the data returned by the IP SLAs UDP operation, the UDP jitter operation can be used as a multipurpose data gathering operation. The packets that IP SLAs generate carry packet sending sequence, receiving sequence information, and sending and receiving time stamps from the source and the operational target. UDP jitter operations can measure the following:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)
- Round-trip delay (average round-trip time)

As the paths for the sending and receiving of data may be different (asymmetric), the per-direction data allow you to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation functions by generating synthetic (simulated) UDP traffic. The UDP jitter operation sends N UDP packets, each of size S, sent T milliseconds apart, from a source switch to a target switch, at a given frequency of F. By default, ten packet-frames (N), each with a payload size of 10 bytes (S), are generated every 10 ms (T), and the operation is repeated every 60 seconds (F). Each of these parameters are user-configurable as shown in the following table.

Table 1: UDP Jitter Operation Parameters

UDP Jitter Operation Parameter	Default	Command
Number of packets (N)	10 packets	**udp-jitter** command, **numpackets** option
Payload size per packet (S)	32 bytes	**request-data-size** command
Time between packets, in milliseconds (T)	20 ms	**udp-jitter** command, interval option
Elapsed time before the operation repeats, in seconds (F)	60 seconds	**frequency (IP SLA)** command

Prerequisites for Configuring IP SLAs UDP Jitter Operations

The prerequisites for configuring IP SLAs UDP jitter operations are as follows:

- Time synchronization, such as that provided by NTP, is required between the source and the target device in order to provide accurate one-way delay (latency) measurements. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data are returned, but values of "0" are returned for the one-way delay measurements provided by the UDP jitter operation.
- Before configuring any IP SLAs application, you can use the **show ip sla application** command to verify that the operation type is supported on your software image.

Guidelines and Limitations for UDP Jitter Operations

- **show** commands with the **internal** keyword are not supported.
- One-way delay (latency) measurements do not support the microsecond unit of measurement. Other units of measurement, such as the millisecond, are 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 2: 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)
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 and Scheduling a UDP Jitter Operation on the Source Device

This section describes how to configure and schedule a UDP jitter operation.

Configuring the IP SLAs Responder on the Destination Device

This section describes how to configure the responder on the destination device.

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

Procedure

	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`	- • (Optional) Temporarily enables the responder functionality on a Cisco device in response to control messages from a source. • (Optional) Required only if protocol control is disabled on a source. Permanently enables the responder functionality on the specified IP addresses and port. Control is enabled by default.
Step 5	**exit** **Example:** `switch(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a Basic UDP Jitter Operation on the Source Device

This section describes how to configure and schedule a basic UDP jitter operation on the source device.

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 sender trace** and **debug ip sla sender error** commands to help troubleshoot issues with an IP SLAs operation.

Procedure

	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 sender** **Example:** `switch(config)# feature sla sender`	Enables the IP SLAs operation feature.
Step 4	**ip sla** *operation-number* **Example:** `switch(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 5	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**sourceport** *port-number*] [**control** { **enable**| **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] **Example:** `switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration submode. Use the **control disable** keyword combination only if you disable the IP SLAs control protocol on both the source and target switches.
Step 6	**frequency** *seconds* **Example:** `switch(config-ip-sla-jitter)# frequency 30`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 7	**exit** **Example:** `switch(config-ip-sla-jitter)# exit`	Exits UDP jitter configuration submode and returns to global configuration mode.
Step 8	**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**] **Example:** `switch(config)# ip sla schedule 5 start-time now life forever`	Configures the scheduling parameters for an individual IP SLAs operation.

	Command or Action	Purpose
Step 9	**exit** **Example:** `switch(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.
Step 10	**show ip sla configuration** [*operation-number*] **Example:** `switch# show ip sla configuration 10`	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

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 helps you to determine whether the service metrics are acceptable.

Configuring and Scheduling a UDP Jitter Operation with Additional Characteristics

This section describes how to configure and schedule a UDP jitter operation with additional characteristics.

- The IP SLAs UDP jitter operation does not support the IP SLAs History feature (statistics history buckets) because of the large data volume involved with UDP jitter operations, which means that the following commands are not supported for UDP jitter operations: **history buckets-kept**, **history filter**, **historylives-kept**, **samples-of-history-kept**, and **show ip sla history**.
- The MIB used by IP SLAs (CISCO-RTTMON-MIB) limits the hours-of-statistics kept for the UDP jitter operation to two hours. Configuring a larger value using the **history hours-of-statistics***hours* global configuration change does not increase the value beyond two hours. However, the Data Collection MIB can be used to collect historical data for the operation. For information, see the CISCO-DATA-COLLECTION-MIB at http://www.cisco.com/go/mibs.

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 sender trace** and **debug ip sla sender error** commands to help troubleshoot issues with an IP SLAs operation.

Before you begin

Before configuring a UDP jitter operation on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco NX-OS software based devices. To enable the responder, perform the task in the “Configuring the IP SLAs Responder on the Destination Device” section.

Procedure

	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 sender** **Example:** `switch(config)# feature sla sender`	Enables the IP SLAs operation feature.
Step 4	**ip sla** *operation-number* **Example:** `Switch(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 5	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets***number-of-packets*] [**interval** *interpacket-interval*] **Example:** `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration submode. • Use the **control disable** keyword combination only if you disable the IP SLAs control protocol on both the source and target switches.
Step 6	**history distributions-of-statistics-kept** *size* **Example:** `Switch(config-ip-sla-jitter)# history distributions-of-statistics-kept 5`	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `Switch(config-ip-sla-jitter)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	**frequency** *seconds* **Example:**	(Optional) Sets the rate at which a specified IP SLAs operation repeats.

	Command or Action	Purpose
	`Switch(config-ip-sla-jitter)# frequency 30`	
Step 9	**history hours-of-statistics-kept** *hours* **Example:** `Switch(config-ip-sla-jitter)# history hours-of-statistics-kept 4`	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 10	**owner** *owner-id* **Example:** `Switch(config-ip-sla-jitter)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 11	**request-data-size** *bytes* **Example:** `Switch(config-ip-sla-jitter)# request-data-size 64`	(Optional) Sets the protocol data size in the payload of an IP SLAs operation's request packet.
Step 12	**history statistics-distribution-interval** *milliseconds* **Example:** `Switch(config-ip-sla-jitter)# history statistics-distribution-interval 10`	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 13	**tag** *text* **Example:** `Switch(config-ip-sla-jitter)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 14	**threshold** *milliseconds* **Example:** `Switch(config-ip-sla-jitter)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 15	**timeout** *milliseconds* **Example:** `Switch(config-ip-sla-jitter)# timeout 10000`	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.

	Command or Action	Purpose
Step 16	**tos** *number* **Example:** `Switch(config-ip-sla-jitter)# tos 160`	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 17	**verify-data** **Example:** `Switch(config-ip-sla-jitter)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 18	**vrf** *vrf-name* **Example:** `Switch(config-ip-sla-jitter)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.
Step 19	**exit** **Example:** `Switch(config-ip-sla-jitter)# exit`	Exits UDP jitter configuration submode and returns to global configuration mode.
Step 20	**ip sla schedule** *operation-number* [**life** {**forever**| *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*] [**recurring**] **Example:** `Switch(config)# ip sla schedule 5 start-time now life forever`	Configures the scheduling parameters for an individual IP SLAs operation.
Step 21	**exit** **Example:** `Switch(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.
Step 22	**show ip sla configuration** [*operation-number*] **Example:** `Switch# show ip sla configuration 10`	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

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 IP SLAs operations, 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 Jitter Operation

This example shows two operations that are configured as UDP jitter operations, with operation 2 starting five seconds after the first operation. Both operations will run indefinitely.

```
feature sla sender
ip sla 1
 udp-jitter 20.0.10.3 65051 num-packets 20
 request-data-size 160
 tos 128
 frequency 30
ip sla schedule 1 start-time after 00:05:00
ip sla 2
 udp-jitter 20.0.10.3 65052 num-packets 20 interval 10
 request-data-size 20
 tos 64
 frequency 30
ip sla schedule 2 start-time after 00:05:05
```

On the target (destination) device:

```
feature sla responder
ip sla responder
```