Configuring IP SLAs UDP Jitter Operations

This document 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 or IPv6 networks. This module also explains how the data gathered using the UDP jitter operation can be displayed and analyzed using Cisco software commands.

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 at the end of this module.

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.

Prerequisites for IP SLAs UDP Jitter Operations

- Time synchronization, such as that provided by the Network Time Protocol (NTP), is required between the source and the target device to provide accurate one-way delay (latency) measurements. To configure NTP on source and target devices, perform the tasks in the "Performing Basic System Management" chapter of the *Basic System Management Configuration Guide*. Time synchronization is not required

for one-way jitter and packet loss measurements. If time is not synchronized between 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 Service Level Agreements (SLAs) application, use the **show ip sla application** command to verify that the operation type is supported on the software image.

Information About IP SLAs UDP Jitter Operations

IP SLAs UDP Jitter Operation

The IP Service Level Agreements (SLAs) UDP jitter operation diagnoses network suitability for real-time traffic applications such as VoIP, video over IP, or real-time conferencing.

Jitter means inter-packet delay variance. When multiple packets are sent consecutively from a source to a destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should receive the packets 10 ms apart. But if there are delays in the network (like 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 packets arrived greater than 10 ms apart. If packets arrive 12 ms apart, then positive jitter is 2 ms; if packets arrive 8 ms apart, negative jitter is 2 ms. For delay-sensitive networks like 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 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 and receiving sequence information, and sending and receiving time stamps from the source and the operational target. Based on this information, UDP jitter operations are capable of measuring 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 paths for sending and receiving data may be different (asymmetric), the per-direction data allows 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. Asymmetric probes support custom-defined packet sizes per direction with which different packet sizes can be sent in request packets (from the source device to the destination device) and in response packets (from the destination device to the source device).

The UDP jitter operation sends N number of UDP packets, each of size S, T milliseconds apart, from a source device to a destination device, at a given frequency of F. In response, UDP packets of size P is sent from the destination device to the source device. 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 is user-configurable, so as to best simulate the IP service that you provide, as shown in the table below.

Table 1: UDP Jitter Operation Parameters

UDP Jitter Operation Parameter	Default	Configuration Commands
Number of packets (N)	10 packets	**udp-jitter num-packets**
Payload size per request packet (S)	10 bytes	**request-data-size**
Payload size per response packet (P)	The default response data size varies depending on the type of IP SLAs operation configured. **Note** If the **response-data-size** command is not configured, then the response data size value is the same as the request data size value.	**response-data-size**
Time between packets, in milliseconds (T)	10 ms	**udp-jitter interval**
Elapsed time before the operation repeats, in seconds (F)	60 seconds	**frequency (IP SLA)**

The IP SLAs operations function by generating synthetic (simulated) network traffic. A single IP SLAs operation (for example, IP SLAs operation 10) repeats at a given frequency for the lifetime of the operation.

How to Configure IP SLAs UDP Jitter 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*

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** *ip-address* **port** *port*
	
	Example:
	
	`Device(config)# ip sla responder`
	
	`Device(config)# ip sla responder udp-echo ipaddress 192.0.2.132 port 5000`
		(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 and port.
		
		• Protocol control is enabled by default.

Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a UDP Jitter Operation on a Source Device

Perform only one of the following tasks:

- Configuring a Basic UDP Jitter Operation on a Source Device
- Configuring a UDP Jitter Operation with Additional Characteristics

Configuring a Basic UDP Jitter Operation on a Source Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **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*]
5. **frequency** *seconds*
6. **end**
7. **show ip sla configuration** [*operation-number*]

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	**ip sla** *operation-number* **Example:** `Device(config)# ip sla 10`	Starts configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*]	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration mode.

	Command or Action	Purpose
	[**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*] **Example:** Device(config-ip-sla)# udp-jitter 192.0.2.135 5000	• Use the **control disable** keyword combination only if you disable the IP SLAs control protocol on both source and destination devices.
Step 5	**frequency** *seconds* **Example:** Device(config-ip-sla-jitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	**end** **Example:** Device(config-ip-sla-jitter)# end	Exits UDP Jitter configuration mode and returns to privileged EXEC mode.
Step 7	**show ip sla configuration** [*operation-number*] **Example:** Device# 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 configure the percentile option for your operation, see the "Configuring the IP SLAs—Percentile Support for Filtering Outliers" module.

Configuring a UDP Jitter Operation with Additional Characteristics

Note
- The IP Service Level Agreements (SLAs) UDP jitter operation does not support the IP SLAs History feature because of the large volume of data involved with UDP jitter operations. This means that the following commands are not supported for UDP jitter operations: **history buckets-kept**, **history filter**, **history lives-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 more information, see the CISCO-DATA-COLLECTION-MIB.

Before You Begin

Before configuring a UDP jitter operation on a 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 IOS software-based devices. To enable the Responder, perform the task in 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-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*]
5. **history distributions-of-statistics-kept** *size*
6. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
7. **frequency** *seconds*
8. **history hours-of-statistics-kept** *hours*
9. **owner** *owner-id*
10. **request-data-size** *bytes*
11. **response-data-size** *bytes*
12. **history statistics-distribution-interval** *milliseconds*
13. **tag** *text*
14. **threshold** *milliseconds*
15. **timeout** *milliseconds*
16. Enter one of the following commands:

    • **tos** *number*

    • **traffic-class** *number*

17. **flow-label** *number*
18. **verify-data**
19. **vrf** *vrf-name*
20. **end**
21. **show ip sla configuration** [*operation-number*]

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	**ip sla** *operation-number* **Example:** Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**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:** Device(config-ip-sla)# udp-jitter 192.0.2.134 5000	Configures the IP SLAs operation as a UDP jitter operation and enters UDP jitter configuration mode. • Use the **control disable** keyword combination only if you disable the IP SLAs control protocol on both source and target devices.
Step 5	**history distributions-of-statistics-kept** *size* **Example:** Device(config-ip-sla-jitter)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop for an IP SLAs operation.
Step 6	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** Device(config-ip-sla-jitter)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 7	**frequency** *seconds* **Example:** Device(config-ip-sla-jitter)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 8	**history hours-of-statistics-kept** *hours* **Example:** Device(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.

	Command or Action	**Purpose**
Step 9	**owner** *owner-id* **Example:** Device(config-ip-sla-jitter)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 10	**request-data-size** *bytes* **Example:** Device(config-ip-sla-jitter)# request-data-size 64	(Optional) Sets the protocol data size in the payload of an IP SLAs operation request packet.
Step 11	**response-data-size** *bytes* **Example:** Device(config-ip-sla-jitter)# response-data-size 25	(Optional) Sets the protocol data size in the payload of an IP SLAs operation response packet.
Step 12	**history statistics-distribution-interval** *milliseconds* **Example:** Device(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:** Device(config-ip-sla-jitter)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 14	**threshold** *milliseconds* **Example:** Device(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:** Device(config-ip-sla-jitter)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 16	Enter one of the following commands: • **tos** *number* • **traffic-class** *number*	(Optional) Defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) Defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.

	Command or Action	Purpose

	Example:
	
	`Device(config-ip-sla-jitter)# tos 160`
	
	`Device(config-ip-sla-jitter)# traffic-class 160`	

Step 17	**flow-label** *number* **Example:** `Device(config-ip-sla-jitter)# flow-label 112233`	(Optional) Defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 18	**verify-data** **Example:** `Device(config-ip-sla-jitter)# verify-data`	(Optional) Causes an IP SLAs operation to check each reply packet for data corruption.
Step 19	**vrf** *vrf-name* **Example:** `Device(config-ip-sla-jitter)# vrf vpn-A`	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) VPNs using IP SLAs operations.
Step 20	**end** **Example:** `Device(config-ip-sla-jitter)# end`	Exits UDP jitter configuration mode and returns to privileged EXEC mode.
Step 21	**show ip sla configuration** [*operation-number*] **Example:** `Device# 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 configure the percentile option for your operation, see the "Configuring the IP SLAs—Percentile Support for Filtering Outliers" module.

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.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 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*]}]	• 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.

	Command or Action	Purpose

	Example:
	
	`Device(config)# ip sla schedule 10 life forever start-time now`
	
	`Device(config)# ip sla 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`	

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.

Verifying IP SLAs UDP Jitter Operations

SUMMARY STEPS

1. **enable**
2. **show ip sla configuration**
3. **show ip sla group schedule**

DETAILED STEPS

Step 1   **enable**
Enables privileged EXEC mode.

> • Enter your password if prompted.

Example:

```
Device> enable
```

Step 2   **show ip sla configuration**
Displays IP SLAs configuration details.

Example:

```
Device# show ip sla configuration

IP SLAs Infrastructure Engine-III
Entry number: 5
Owner: ownername
Tag: text
Operation timeout (milliseconds): 9999
Type of operation to perform: udp-jitter
Target address/Source address: 192.0.2.115/0.0.0.0
Target port/Source port: 5/0
Type Of Service parameter: 0x5
Request size (ARR data portion): 100
Response size (ARR data portion): 200
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Operation Stats Precision : microseconds
Timestamp Location Optimization: enabled
Operation Packet Priority : high
NTP Sync Tolerance : 0 percent
Vrf Name:
Control Packets: enabled
```

Step 3   **show ip sla group schedule**
Displays IP SLAs group schedule details.

Example:

```
Device# show ip sla group schedule
```

```
Group Entry Number: 1
Probes to be scheduled: 6-9,3-4
Total number of probes: 6
Schedule period: 10
Mode: even
Group operation frequency: Equals schedule period
Status of entry (SNMP RowStatus): Active
Next Scheduled Start Time: Pending trigger
Life (seconds): 3600
Entry Ageout (seconds): never
```

Configuration Examples for IP SLAs UDP Jitter Operations

Example: Configuring a UDP Jitter Operation

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

```
configure terminal
 ip sla 1
  udp-jitter 192.0.2.115 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 192.0.2.115 65052 num-packets 20 interval 10
  request-data-size 20
  tos 64
  frequency 30
 ip sla schedule 2 start-time after 00:05:05
```

Enter the following command on the target (destination) device to temporarily enable the IP SLAs responder functionality on a Cisco device in response to control messages from the source device.

```
ip sla responder
```

Additional References for IP SLAs UDP Jitter Operations

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference

MIBs

MIBs	MIBs Link
• CISCO-DATA-COLLECTION-MIB • CISCO-RTTMON-MIB • IPV6-FLOW-LABEL-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 IP SLAs UDP Jitter Operations

Table 2: Feature Information for the IP SLAs UDP Jitter Operation

Feature Name	Releases	Feature Information
IP SLAs—UDP Jitter Operation		The IP SLAs 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.
IP SLAs for IPv6 (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)		The IP SLAs for IPv6 (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect) feature adds support for operability in IPv6 networks.

Feature Name	Releases	Feature Information
IP SLAs—Asymmetric Probe Support for UDP Jitter		The IP SLAs—Asymmetric Probe Support for UDP Jitter feature supports the configuration of custom-defined packet sizes in response packets. The following command was introduced: **response-data-size**.