



Configuring Cisco IP SLAs ICMP Jitter Operations

This module describes how to configure a Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Jitter operation for generating a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics. The destination device can be any network device that supports ICMP such as a server or workstation. Available statistical measurements for IP SLAs ICMP jitter operations include latency, round-trip time, jitter (interpacket delay variance), and packet loss. The IP SLAs ICMP jitter operation does not require an IP SLAs Responder on the destination device.

- [Finding Feature Information, page 1](#)
- [Restrictions for IP SLAs ICMP Jitter Operations, page 1](#)
- [Information About IP SLAs ICMP Jitter Operations, page 2](#)
- [How to Configure IP SLAs ICMP Jitter Operations, page 3](#)
- [Configuration Examples for IP SLAs ICMP Jitter Operations, page 8](#)
- [Additional References, page 9](#)
- [Feature Information for IP SLAs - ICMP Jitter Operation, page 10](#)

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 ICMP Jitter Operations

- Cisco IOS-XR devices do not support ICMP Timestamp and hence all ICMP jitter operations to these devices fail.

- When compared to the IP SLAs User Datagram Protocol (UDP) jitter operation, the IP SLAs ICMP jitter operation may provide less accurate measurements because the accuracy of the measurements provided by a non-Cisco destination device cannot be determined.
- Because ICMP packets do not support voice technology, the IP SLAs ICMP jitter operation does not support Mean Opinion Score (MOS), Calculated Planning Impairment Factor (ICPIF), or estimated transmission rating factor (R) reaction configuration capabilities.

Information About IP SLAs ICMP Jitter Operations

Benefits of the IP SLAs ICMP Jitter Operation

The IP SLAs ICMP Jitter Operation feature provides the following key benefits:

- End-to-end performance measurements between a Cisco device (source) and any other IP device (destination) using ICMP.
- Proactive threshold violation monitoring through Simple Network Management Protocol (SNMP) trap notifications and syslog messages.

Statistics Measured by the IP SLAs ICMP Jitter Operation

The IP SLAs ICMP jitter operation supports the following statistical measurements:

- Jitter (source-to-destination and destination-to-source)
- Latency (source-to-destination and destination-to-source)
- Round-trip time latency
- Packet loss
- Successive packet loss
- Out-of-sequence packets (source-to-destination, destination-to-source, and round-trip)
- Late packets

IP SLAs ICMP jitter uses a two ICMP time stamp messages, an ICMP Timestamp Request (Type 13) and an ICMP Timestamp Reply (Type 14), to provide jitter, packet loss, and latency. IP SLAs ICMP jitter operations differ from IP SLAs ICMP echo operations in that ICMP echo uses ICMP Echo request and reply (ping). Devices that are fully compliant with RFC 792, *Internet Control Message Protocol*, must be able to respond to the time stamp messages without requiring an IP SLA responder at the destination.

**Note**

Cisco IOS devices support RFC 792's timestamp requests and replies, but Cisco IOS-XR devices do not support this.

The ICMP API sends a configurable number of request message packets out of the interface. The data (time stamp) that is received in the request is returned in a reply message packet along with another time stamp.

Every packet includes three time stamps: an Originate (sent) Timestamp, a Receive Timestamp, and a Transmit (reply) Timestamp.

IP SLAs utilizes the time stamps to calculate jitter for each direction, based on the difference between interarrival and interdeparture delay for two successive packets. If the difference is positive, it is counted in positive jitter. A negative value is counted in negative jitter. Separate measurements for the source-to-destination and destination-to-source data paths can be used to identify problems in your network because the paths can be different (asymmetric).

Each ICMP packet includes a sequence number in its header that is used to count the number of packets received out of sequence on the sender. Both the sequence number and the receive timestamps can be used to calculate out-of-sequence packets on the source-to-destination path. If the receive time stamp for a packet is greater than that of the next packet, the first packet was delivered out of order on the source-to-destination path. For the destination-to-source path, the same method can be applied. Note that if the packet is out of order on the source-to-destination path, it should be returned out of order to the sender unless there is also misordering on the destination-to-source path.

If any packet cannot be sent due to an internal or unexpected error, or because the timerwheel slot containing the packet is missed, it is counted as Packet Skipped. This metric is very important because statistics are measured on sent packets only.

All timed-out packets are counted towards Packet Loss. Successive packet loss is calculated by counting, and adding, the number of successive dropped packets. Successive packet loss is reported as minimum of successive packet drop and maximum of successive packet drop.

All other statistics are calculated using the same logic as a UDP jitter operation.

How to Configure IP SLAs ICMP Jitter Operations

Configuring an IP SLAs ICMP Jitter Operation

**Note**

This operation does not require an IP SLAs Responder on the destination device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-jitter** {*destination-ip-address* | *destination-hostname*} [**interval** *milliseconds*] [**num-packets** *packet-number*] [**source-ip** {*ip-address* | *hostname*}]
5. **frequency** *seconds*
6. **history** *history-parameter*
7. **owner** *owner-id*
8. **tag** *text*
9. **threshold** *milliseconds*
10. **timeout** *milliseconds*
11. **tos** *number*
12. **vrf** *vrf-name*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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	icmp-jitter { <i>destination-ip-address</i> <i>destination-hostname</i> } [interval <i>milliseconds</i>] [num-packets <i>packet-number</i>] [source-ip { <i>ip-address</i> <i>hostname</i> }] Example: Device(config-ip-sla)# icmp-jitter 172.18.1.129 interval 40 num-packets 100 source-ip 10.1.2.34	Configures the IP SLAs operation as an ICMP jitter operation and enters IP SLAs ICMP jitter configuration mode.

	Command or Action	Purpose
Step 5	<p>frequency <i>seconds</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# frequency 30</pre>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	<p>history <i>history-parameter</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# history hours-of-statistics-kept 3</pre>	(Optional) Specifies the parameters used for gathering statistical history information for an IP SLAs operation.
Step 7	<p>owner <i>owner-id</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# owner admin</pre>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 8	<p>tag <i>text</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# tag TelnetPollServer1</pre>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 9	<p>threshold <i>milliseconds</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# threshold 10000</pre>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 10	<p>timeout <i>milliseconds</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# timeout 10000</pre>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 11	<p>tos <i>number</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# tos 160</pre>	(Optional) Defines a type of service (ToS) byte in the IP header of an IP SLAs operation.
Step 12	<p>vrf <i>vrf-name</i></p> <p>Example:</p> <pre>Device(config-ip-sla-icmpjitter)# vrf vpn-A</pre>	(Optional) Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using IP SLAs operations.

	Command or Action	Purpose
Step 13	end Example: Device(config-ip-sla-icmpjitter)# end	Exits to privileged EXEC mode.

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	<p>enable</p> <p>Example:</p> <pre>Device> 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>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>Enter one of the following commands:</p> <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> 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>]}] <p>Example:</p> <pre>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</pre>	<ul style="list-style-type: none"> • 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	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>
Step 5	<p>show ip sla group schedule</p> <p>Example:</p> <pre>Device# show ip sla group schedule</pre>	<p>(Optional) Displays IP SLAs group schedule details.</p>

	Command or Action	Purpose
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 ICMP Jitter Operations

Example Configuring an IP SLAs ICMP Jitter Operation

The following example shows how to configure an IP SLAs ICMP jitter operation:

```
ip sla 10
 icmp-jitter 172.18.1.129 interval 40 num-packets 100 source-ip 10.1.2.34
 frequency 50
!
ip sla reaction-configuration 1 react jitterAvg threshold-value 5 2 action-type trap
 threshold-type immediate
!
ip sla schedule 1 start-time now life forever
```


Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS IP SLAs commands	IP SLAs Command Reference
Cisco IOS IP SLAs: general information	Cisco IOS IP SLAs Overview chapter of the <i>Cisco IOS IP SLAs Configuration Guide</i> .

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-RTTMON-MIB • CISCO-RTTMON-ICMP-MIB 	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 792	<i>Internet Control Message Protocol</i>

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 - ICMP Jitter 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 IP SLAs - ICMP Jitter Operation

Feature Name	Releases	Feature Information
IP SLAs ICMP Jitter Operation	12.4(6)T Cisco IOS XE Release 3.8S	The Cisco IOS IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) jitter operation provides the capability to generate a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics. Available statistical measurements for the IP SLAs ICMP jitter operation include latency, round-trip time, jitter (interpacket delay variance), and packet loss.